AGRC Certificate in AML

Study Pack

Table of Contents

About AGRC 1

PAGRC -The AGRC Professional level Certifications 1

Chapter 1 2

Money Laundering and Terrorist Financing 2

Learning Objectives 2

Introduction 2

1. Understanding Money Laundering and Terrorist Financing 2

1.1 The global extent of the Problem 2

1.2 Macroeconomic consequences 3

1.3 The three basic stages of Money Laundering 5

1.4 Financing of Terrorism 8

1.5 The use of non-profit organisations in Terrorist Financing 11

2. Money Laundering and Terrorist Financing 11

2.1 Similarities between money laundering and terrorist financing 11

2.2 Differences between money laundering and terrorist financing 11

2.3 Criminalisation of money laundering and other offences 13

3. Learning summary 16

4. End of Chapter Questions 16

Chapter 2 19

AML Supervision 19

Learning Objectives 19

Introduction 19

1. Bodies to Combat Money Laundering and Terrorist Financing 20

1.1 The FATF 20

1.2 EUROPEAN COMMISSION 21

1.3 MONEYVAL 21

1.4 The BASEL Committee 22

1.5 The Wolfsberg Group 23

1.6 The Egmont Group 23

2. Global AML Standards 24

2.1 The FATF 40 recommendations 24

2.2 The European Directives 25

2.3 The 4th AML directive 25

2.4 The 5th AML Directive 31

2.5 The 6th AML Directive 33

3. Learning Summary 34

4. End of Chapter Questions 35

Chapter 3 38
The AML Compliance Program 38
Learning Objectives 38
Introduction 38
1. Elements of a successful AML Compliance Program 39
1.1 The Board of Directors 39
1.2 The Internal Audit Function 40
1.3 The Money Laundering Compliance Officer (MLCO) 41
1.4 Employees obligations, training, and Ongoing Awareness 42
2. Establishing an acceptable risk policy 43
2.1 Client Acceptance Policy 43
2.2 Establishing appropriate policies and procedures 44
3. Learning summary 45
4. End of Chapter Questions 45
Chapter 4 48
The risk-based approach 48
Learning Objectives 48
Introduction 48
1. Understanding risks 49
1.1 The EU Supranational Risk Assessment 49
1.2 National Risk Assessments 49
1.3 The importance of RBA 50
1.4 Application of the RBA 51
1.5 Business-wide risk assessments 51
1.6 Identification of ML risks on business relationships 52
1.7 Customer Risk Assessment 54
1.8 The risk-based approach in terrorist financing 55
2. Risk factors 55
2.1 Risk-Based Approach risk factors 56
3. Risk Management 62
3.1 Risk management treatment 63
4. Customer classification 64
4.1 AML/CFT Risk Scoring 64
4.2 Weighting of risk factors 67
5. Learning summary 68
6. End of Chapter Questions 68
Chapter 5 71
Customer Due Diligence (CDD) 71
Learning objectives 71

Introduction 71
1. Know Your Customer (KYC) and Customer Due Diligence (CDD) 72
1.1 When is KYC and CDD applied? 73
1.2 Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures 73
1.3 Customer Onboarding and Know Your Customer (KYC) 75
2. Simplified and Enhanced Due Diligence measures 78
2.1 Simplified due diligence (SDD) 78
2.2 Enhanced Due Diligence (EDD) 80
2.3 Application of EDD measures 83
3. Other CDD Obligations 84
3.1 Record keeping requirements and data retention 84
3.2 Monitoring of transactions 85
3.3 Suspicious Transaction/Activity Reporting (STR/SAR) 87
3.4 Reporting of suspicious transactions in EU and the US 89
3.5 Implementation of KYC standards in a cross-border context 90
4. Learning summary 92
5. End of Chapter Questions 92
Chapter 6 95
SANCTIONS 95
Learning Objectives 95
Introduction 95
1. Understanding Sanctions 96
1.1 Key Definitions 96
1.2 Forms of Sanctions 96
1.3 Categories of Sanctions 96
1.4 Primary Vs Secondary Sanctions 98
1.5 When are sanctions successful? 99
2. Sanction Lists 101
2.1 United Nations Sanctions 101
2.2 The European Union Sanctions 102
2.3 Unilateral Sanctions: The case of the US 106
2.4 Why does the US issue sanctions unilaterally? 107
2.5 US Decision-Making Framework 108
2.6 Administration of Sanctions Programme – Who executes the President's decisions? 112
2.7 OFAC's 50 Per Cent Rule for Entities 113
2.8 Other important and relevant agencies in the Executive Branch: 114
3. Sanctions Compliance Strategy 115
3.1 Sanctions Risk Assessment 116
4. Learning Summary 121

5. End of Chapter Questions 122
Chapter 7 125
Vulnerabilities of Financial Institutions to ML and TF 125
Learning Objectives 125
Introduction 125
1. Vulnerabilities of banking services to money laundering and terrorist financing 126
1.1 Wealth Management 126
1.2 Correspondent banking 127
1.3 Lending and Credit Facilities 128
1.4 Investment Banking 128
1.5 International Trade Finance 129
2. Other sectors 130
2.1 Insurance Products 130
2.2 The Securities Sector 130
2.3 Digital or Virtual Currencies 132
2.4 Money transfer and foreign exchange bureaus 133
3. Learning summary 134
4. End of Chapter Questions 134
Chapter 8 137
Money Laundering and Terrorist Financing Case Studies 137
Introduction 137
1. Danske Bank AML Case study 137
2. Swedbank case study 143
Chapter 9 148
Glossary of Terms 148
Chapter 10 159
Practice Questions 159
Reference Materials 168
1. AML Global Organisations 168
2. Useful Resources 174

About AGRC

The Association of Governance, Risk and Compliance (AGRC) is a non-for-profit global professional accreditation and certification organisation, as well as a networking platform. We aim to facilitate the exchange of knowledge and sharing of experiences among compliance, risk, cybersecurity, and governance professionals. At AGRC, we aspire to continuously grow our community of professionals to ensure multi-jurisdictional regulatory compliance in financial services and to share values, experience, expertise and opportunities.

The AGRC mission is to improve the integrity of the global financial services industry by:

- Providing access to a globally recognised certification and continuous education programmes that will enable the compliance, risk, cybersecurity, technology and governance community to improve effectiveness and support businesses
- Offering a valuable forum for professionals from all over the world, focusing on how the latest developments on compliance, risk, cybersecurity and governance may improve the efficiency and effectiveness of organisations
- Sharing information and offering insights and support to provide knowledge for best industry practices
- Facilitating the exchange of ideas, knowledge and experience by holding annual conferences, expanding member networks, creating high value content and increasing the visibility of our work in the financial and other industry sectors

To achieve its mission AGRC:

- Promotes global and harmonized standards with regards to laws and regulation relating to compliance, risk, cybersecurity, technology and governance
- Engages in dialogue with relevant authorities and institutions
- Educates professionals in the private and public sector organisations about set standards and the strategies and practices required to meet them
- Certifies the achievements of its members
- Provides a networking platform for collaboration and peer to peer learning amongst members throughout the world

PAGRC -The AGRC Professional level Certifications

The Governance, Risk and Compliance Professional (PAGRC) certification ensures that an individual has the skills and technical knowledge required to perform the duties of a AML professional, governance-related officer, risk manager, cybersecurity officer and compliance officer or internal auditor role within an organisation. PAGRC is the foundation for all other Certifications. This Certificate is suitable for every AML, compliance, risk, finance, internal audit and IT professional operating within a regulated environment.

Chapter 1

Money Laundering and Terrorist Financing

Learning Objectives

- The basic stages of money laundering
- Methods used in money laundering
- Financing of terrorism
- Similarities and differences between money laundering and terrorist financing

Introduction

The broadly accepted definition of money laundering is: "The process by which criminals seek to conceal the true origins and/or ownership of the proceeds, or benefits, of criminal activity".

Illegal arms sales, smuggling, organised crime, drug trafficking, prostitution and other illegal activities can generate huge amounts of proceeds.

The aim of the process is to achieve a situation where the proceeds of the illegal activities appear legitimate. This can enable criminals to avoid prosecution, conviction, and the confiscation of the criminal funds. Criminals use financial institutions as the major conduits to assist in these activities. This means that it is important that those working in the financial services sector are fully aware of the regulatory requirements in respect of money laundering, and of their personal responsibilities.

In this Chapter we will examine the consequences of money laundering, the basic stages and the methods used by criminals to launder illicit funds. We will also see the similarities and differences between money laundering and terrorist financing.

1. Understanding Money Laundering and Terrorist Financing

1.1 The global extent of the Problem

The clandestine nature of money laundering makes it difficult to produce an accurate estimate of the total amount of money being laundered each year. Estimates suggest that in excess of a staggering US $1 trillion per year is being laundered by financial criminals, drug dealers and arms traffickers worldwide. This figure is in line with United Nations Office on Drugs and Crime (UNODC) estimates.

Given the scale of the problem it is not surprising that AML policies and actions are high on the international agenda and combating this issue continues to be a major challenge for the financial sector globally. Increasingly, AML provisions are being seen as the frontline in the battle against drug dealing, organised crime, and the financing of terrorism. Much law enforcement activity is directed towards making the disposal of criminal assets more difficult, monitoring the movement of assets and the seizure, or freezing of those assets where possible.

DID YOU KNOW?
The United Nations Office on Drugs and Crime (UNODC) estimates that between US $800 billion and US $2 trillion is laundered globally each year.

1.2 Macroeconomic consequences

Money laundering poses significant threats to the integrity of the global financial system and enables financial crime. Funds generated through drugs, human trafficking, tax evasion and other crimes have the following consequences:

Increased Exposure to Organised Crime and Corruption: Successful money laundering enhances the profitable aspects of criminal activity. When a country is seen as a heaven for money laundering, it will attract people who commit crime.

Undermining the Legitimate Private Sector: One of the most serious macroeconomic effects of money laundering is felt in the private sector.

Weakening Financial Institutions: Money laundering and terrorist financing can harm the soundness of a country's financial sector. They can negatively affect the stability of individual banks or other financial institutions, such as securities firms and insurance companies. Criminal activity has been associated with a number of bank failures around the globe, including the closures of internet bank, European Union Bank[1], as well as Riggs Bank. The establishment and maintenance of an effective AML/CFT program is usually part of a financial institution's charter to operate; non-compliance can result not only in significant civil money penalties, but also in the loss of its charter.

Dampening Effect on Foreign Investments: Although developing economies cannot afford to be too selective about the sources of capital they attract, there is a dampening effect on

[1] The European Union Bank was initially registered as an offshore bank in Antigua in 1994 and was set up by two Russian nationals with a dubious background. In September 1995 it launched its website and claimed to be the first Internet bank. Its target audience included individuals that aimed to find a heaven for 'dirty' money and avoid taxes and strict regulation and it was a matter of time before it came under the radar of regulatory bodies. The bang collapsed in 1997 amidst warnings and investigations regarding its operations. (source: https://www.imolin.org/imolin/finhaeng.html)

foreign direct investment when a country's commercial and financial sectors are perceived to be compromised and subject to the influence of organised crime. To maintain a business-friendly environment this resistance must be weeded out.

Loss of Control of, or Mistakes in, Decisions Regarding Economic Policy: Due to the large amounts of money involved in the money laundering process, in some emerging market countries these illicit proceeds may dwarf government budgets. This can result in the loss of control of economic policy by governments or in policy mistakes due to measurement errors in macroeconomic statistics.

Economic Distortion and Instability: Money launderers are not primarily interested in profit generation from their investments, but rather, in protecting their proceeds and hiding the illegal origin of the funds. Thus, they "invest" their money in activities that are not necessarily economically beneficial to the country where the funds are located. Furthermore, to the extent that money laundering and financial crime redirect funds from sound investments to low-quality investments that hide their origin economic growth can suffer.

Loss of Tax Revenue: Among the underlying forms of illegal activity, tax evasion is, perhaps, the one with the most obvious macroeconomic impact. Money laundering diminishes government tax revenue and therefore, indirectly harms honest taxpayers. It also makes government tax collection more difficult. This loss of revenue generally means higher tax rates than would normally be the case.

Risks to Privatisation Efforts: Money laundering threatens the efforts of many states trying to introduce reforms into their economies through the privatisation of state-owned properties such as land, resources, or enterprises. Sometimes linked with corruption or inside deals, a government may award a state privatisation tender to a criminal organisation potentially at an economic loss to the public.

Reputation Risk for the Country: A reputation that a country is a money laundering or terrorist financing heaven can harm development and economic growth in a country.

Risk of International Sanctions: In order to protect the financial system from money laundering and terrorist financing, the United States, the United Nations, the European Union (EU), and other governing bodies may impose sanctions against foreign countries, entities or individuals, terrorists and terrorist groups, drug traffickers, and other security threats. In the United States, the Office of Foreign Assets Control (OFAC) of the US Department of the Treasury administers enforces economic and trade sanctions.

Social Costs: Significant social costs and risks are associated with money laundering. Money laundering is integral to maintaining the profitability of crime. It also enables drug traffickers, smugglers, and other criminals to expand their operations. This drives up the cost of government expenses and budgets due to the need for increased law enforcement and other expenditures (for example, increased healthcare costs for treating drug addicts) to combat the serious consequences that result.

Reputational Risk of organisations: The potential that adverse publicity regarding an organisation's business practices and associations, whether accurate or not, will cause a loss

of public confidence in the integrity of the organisation. As an example, reputational risk for a bank represents the potential that borrowers, depositors, and investors might stop doing business with the bank because of a money laundering scandal.

Given the scale of the problem, it is not surprising that AML policies and actions are high on the international agenda and combating this issue continues to be a major challenge for the financial sector globally. Increasingly, AML provisions are the frontline in the battle against drug dealing, organised crime, and the financing of terrorism. Many of the law enforcement activities are directed towards making the disposal of criminal assets more difficult, monitoring the movement of assets and the seizure, or freezing of those assets possible.

1.3 The three basic stages of Money Laundering

After a crime is committed, the illegal funds derived from the specific crime need to enter the financial system in a way that it will not raise any suspicions for the underlying crime. Money laundering is usually performed in three basic stages.

Placement is the physical introduction of cash or other proceeds into the financial system – for example, by depositing cash into a bank account. Other ways of placing physical cash derived from criminal activities into the financial system include:

- commingling of illegitimate with legitimate funds using cash-intensive business such a nail bar, hair saloon or local restaurant,
- purchasing currency from a foreign exchange office using cash earned from illegal activity,
- structuring of deposits by placing small sums of cash into numerous bank accounts,
- repaying legitimate loans using cash earned from illegal activity,
- purchasing prepaid cards from a merchant using cash earned from illegal activity.

A method that criminals often use to place their illegitimate funds into the financial system is "smurfing", an action where the cash derived from a crime is divided into small amounts and then an individual (a "smurf") is contracted to use these smaller tranches and carry out a financial transaction, such as a deposit, under the reporting threshold, without raising suspicion. "Smurfs" are also used to currency smuggling by moving physical cash cross-border and purchasing foreign exchange with illegal funds.

Another method used by criminals to launder their illicit funds is known as "reverse flip". This is where a money launderer buys a property at a reported purchase price much lower than the actual value of the property and then pays the difference "under the table". Then the launderer he may sell the property at the actual value and gets clean funds from the purchaser.

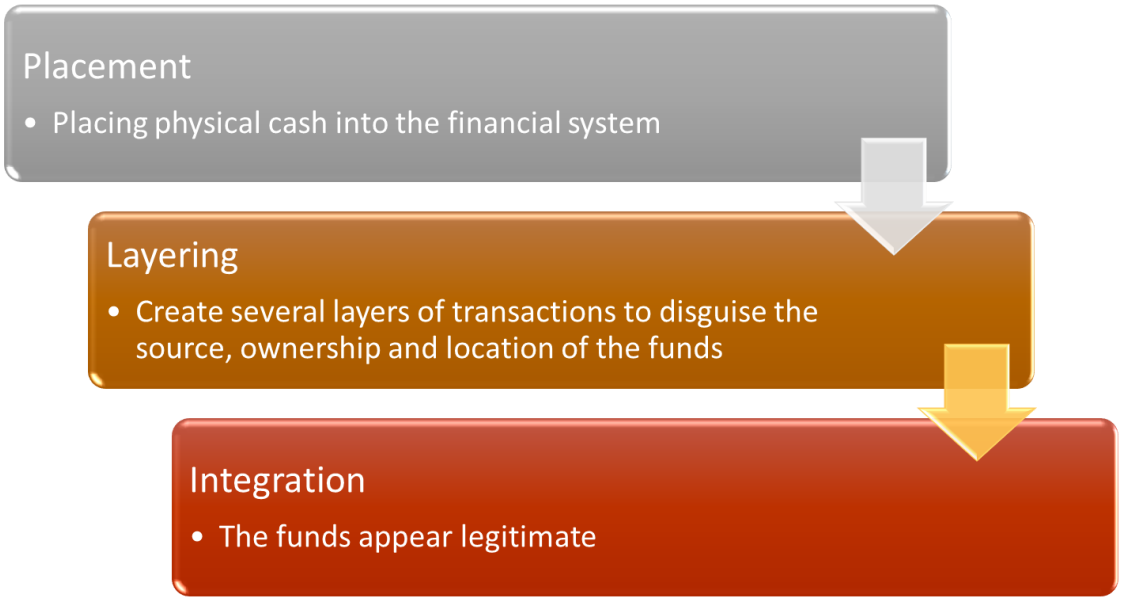
Layering is the second stage of money laundering. It is the process of moving the proceeds through a number of financial transactions, in many cases complex transactions, so as to make the audit trail more difficult to trace back and make it difficult for the authorities to link the funds with the initiator of the money laundering scheme. Examples include:

- selling one investment and reinvesting in another,
- moving the money between different institutions or jurisdictions,
- setting up investment vehicles such as holding companies or trusts with the purpose to hide the real owner of the assets,
- purchasing of cryptocurrency using funds deposited into a bank account.

Integration is the last stage of money laundering. It is very difficult to detect money laundering in the integration stage. The reason for that is that the funds have been sufficiently distanced from their origin and have achieved the appearance of legitimacy. The money is integrated into the normal economy and now belong to the initiator of the money laundering scheme. In the integration stage criminals at this stage:

- Invest in real estate
- purchase cars, jewellery, fine art, or other high value items,
- invest in a legitimate business through purchase of shares or provision of loans.

It is important to note that it is not necessary for all three of these steps to occur for money laundering to have taken place. Sometimes, a criminal may place proceeds into the financial system and then integrate them, using the funds to purchase a vehicle or fund the purchase of a house. In other cases, the crime may involve defrauding consumers by convincing them to invest in illicit investment schemes and transferring funds to other accounts already controlled by the criminals involved. In this case, the placement stage is not present as the funds are already inside the financial system. However, the criminals would still need to layer or disguise the trail of the funds (where those funds came from) before they can use them down the line. In addition, the boundaries between the stages may be blurred or overlap and, in some cases, they may occur simultaneously (though this is not common). Below, two case studies are reviewed to better illustrate how money laundering can take place:


Placement
• Placing physical cash into the financial system
Layering
• Create several layers of transactions to disguise the source, ownership and location of the funds
Integration
• The funds appear legitimate

Case Study

A drug trafficker, El Nata, was based in the southern Spanish province of Granada. He was selling and transporting marijuana and, El Nata and his crew accumulated a fortune close to €8 million (including assets, property, and cash) that allowed them to lead a life of luxury and excess.

In August 2020, the Spanish Civil Guard working closely with the Polish Police Central Bureau of Investigation and Europol carried out carried out operation 'Vangelis' and seized over €8 million worth of criminal assets and arrested 75 suspects.

The drugs were grown and sold throughout Europe. Criminal assets included a total of 36 properties and 50 vehicles, valued at over €8 million, as well as close to €200 000 in cash were seized. A further €370 000 was blocked on the criminals' bank accounts.

With the reference to the three stages of Money Laundering, El Nata was laundering money in the following stages:

- Placement: Cash proceeds from sales deposited into bank accounts
- Layering: Possible transfers between bank accounts controlled by the criminals
- Integration: Purchase of properties and vehicles using either cash or bank transfers

Source Europol (Link)

Case Study

In July 2018, Europol supported the Spanish Guardia Civil and the National Police of Colombia in dismantling two criminal organisations involved in large-scale money laundering across Europe and South America. It is estimated that 2.5 million euros were laundered by using different methods, such as smurfing and cryptocurrency exchanges.

The illicit organisations involved in the scheme helped other criminals launder the proceeds earned from their illegal activities. Criminals would provide them with their cash, which would then be split up in small remittances ("smurfing"). In other cases, the group used cryptocurrency exchanges to convert large amounts of money from cash into cryptocurrencies, like Bitcoins and Altcoins, and later transferred them to other virtual wallets controlled by the criminal organisation, which allowed the return of the illicit proceeds to South America, thus hiding the origin of the money.

- Placement: Smurfing. Cash from an illegal source was divided into small amounts and then various individuals, "smurfs", were contracted to use these smaller tranches and carry out deposits without raising suspicion.

- Layering: Use of exchanges; purchase of crypto currency; use of e-wallets

- Integration: Illicit proceeds were returned to South America to purchase assets or

other types of investments

Source: Europol (Link)

The three stages of money laundering are mainly used for cash-based crime, such as drugs or people trafficking, prostitution or armed robbery from banks. It does not cover the increasing range of criminal activity and invention. Laundering does not have to involve money at all, since the proceeds to be laundered can involve any sort of tangible or intangible property derived from crime. It is also the case that criminal property does not have to move for it to be laundered. For example, legitimately earned money that has not been declared for tax may be placed directly into a bank account in a different jurisdiction from where it was earned. At this point, it represents the profit from a legitimate activity but, because it has not been declared for tax in the jurisdiction in which it was earned, it becomes the proceeds of a crime.

Similarly, the proceeds of fraud, bribery, corruption and insider dealing often involve the use and abuse of private limited companies and trusts set up in jurisdictions well away from the scenes of these crimes. In this way corrupt officials and criminals seek to distance the criminality from which they wish to avoid detection by arrangements designed to disguise the true ownership of those vehicles.

Consequently, in most jurisdictions anti-money laundering (AML) laws are aimed at identifying personal customers and the ultimate beneficial ownership of corporate customers, monitoring transactions, keeping good records and reporting suspicions to the authorities. The purpose is to enable obliged entities to identify suspicions for funds derived from illegal activities.

1.4 Financing of Terrorism

After the 9/11 terrorist attacks in New York and the terrorism-related attacks that followed in Europe, the subject of terrorist financing has also remained high on the international political agenda. Combating terrorist financing has been viewed as one of the most critical fronts in the war on terror and continuing geopolitical events show that this topic remains in sharp focus.

Terrorist activities are increasingly global and there is a strong need for international co-operation. Governments are also being encouraged to take all possible measures to ensure that they do not provide safe havens for individuals charged with the financing of terrorism, and to have procedures in place to extradite, where possible, such individuals. They are also encouraged to afford other countries the greatest possible measure of assistance in connection with criminal, civil enforcement and administrative investigations, inquiries and proceedings relating to the financing of terrorism.

The FATF Recommendation 5 requires countries to extend the terrorist financing offences to any person who wilfully provides or collects funds or other assets by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are used, in full or in part:

a. To carry out a terrorist act
b. By a terrorist organisation or

c. By an individual terrorist

Terrorist financing offences extend to any funds or other assets, whether from a legitimate or illegitimate source. Although each country is required to implement measures for combatting financing of terrorism, there are some common types of activities that can be prosecuted as a terrorism offence include:

- Threat to commit a terrorist act
- Participation in a terrorist group
- Providing any type of support to a terrorist group or terrorists
- Get trained or receiving instructions for acts of terrorism with the purpose to commit a terrorist act
- Theft, extortion and forgery associated with a terrorist offence
- Refusal to disclose information
- Distribution of messages to the public, either through the internet or other means that support the commission of a terrorist act
- Intentionally motivates another person to engage with committing a terrorist act
- Travel for the purpose of committing a terrorist act
- Assists another person to travel with the purpose of committing a terrorist act
- Initiate, attempt or cooperate with others to commit a terrorist act.

The controls that are applied to disrupt attempts to finance terrorism-related activities are just as important as the detection and prevention of money laundering. Many of the requirements of national and international anti-terrorism legislation on financial services firms are similar to the AML provisions and involve customer identification, transaction monitoring, record keeping and reporting of suspicious activity.

Case Study

Al-Shabaab - Somali al-Qaida-affiliated movement

The organisation has developed highly effective tax, fundraising and payment systems to sustain itself and the welfare it provides based on the 'financial control and surveillance of cashflows', involving both domestic and external sources.

In contrast to other groups that benefit from the availability of 'lootable' and 'unlootable' resources such as diamonds, narcotics, oil and gas in a territory they control, Al-Shabaab does not uses these sources of funding. Instead, it has developed a highly diversified and innovative funding model, which relies on the 'financial control and surveillance of cashflows' and involves both domestic and external sources, much of which is within its control and not heavily reliant on third parties.

According to the UN, in 2011 Al-Shabaab's annual revenue was in the region of $70–100 million stemming from 'duties and fees levied at airports and seaports, taxes on goods and services, taxes in kind on domestic produce, jihad contributions, checkpoints and various forms of extortion justified in terms of religious obligations, or zakat'. Zakat is an Islamic religious tithe.

In brief, Al-Shabaab operates a vetting and registration system that includes the requirement of aid agencies to pay fees of up to $10,000 to operate and distribute aid. Once an aid agency has been assessed by an Al-Shabaab Humanitarian Coordination Officer, further taxes and measures might be demanded based on the nature of the aid being distributed or type of project being undertaken.

Source: Keatinge, Tom, and Royal United Services Institute for Defence and Security Studies. *The role of finance in defeating Al-Shabaab*. RUSI, 2014.

Case Study

It was a counterterrorism investigation with an unusual twist—the suspect in an FBI Baltimore case was on the receiving end of money being transmitted into the United States from foreign terrorism operatives overseas, to help him plan a terrorist attack in America.

Mohamed Elshinawy pleaded guilty, admitting to conspiring with others to provide material support and resources to ISIS and engaging in terrorist activity. In March of this year, he was sentenced to 20 years in federal prison.

The case began in June 2015, when the FBI became aware of an individual located in Egypt wiring $1,000 to a 30-year-old newspaper deliveryman who resided in Edgewood, Maryland. The recipient on the same day drove to his local bank branch and deposited most of it.

After several lies to the FBI, he finally said that he began communicating with the ISIS, who wired him several payments totalling about $4,000 for "operational purposes", which, as Elshinawy believed, were to be used for some sort of terrorist attack on U.S. soil. As a cover for these payments he was receiving from ISIS, Elshinawy set up a scheme pretending to sell printers online. But according to Elshinawy, he never intended to carry out any attack and was just scamming money from the terrorist group.

The FBI investigations uncovered that Elshinawy had previously pledged his allegiance to ISIS during social media discussions, described himself as a soldier dedicated to carrying out violent jihad, and asked his childhood friend to convey his message of loyalty to ISIS leadership. He also asked for guidance on how to obtain or make an explosive device and a silencer, bought multiple pay-as-you-go phones and a laptop and used a virtual private network to communicate incognito with his contacts abroad, and tried recruiting his brother—who was living in Saudi Arabia at the time—into ISIS.

Soon after his interviews with the FBI, Elshinawy began taking steps to erase his communications and advised co-conspirators to do the same.

Elshinawy's plan to accept money to fund a terrorist attack in the U.S. was not a standalone plot—it led to the uncovering of a broader conspiracy involving an international ISIS financing network, shady shell companies[2], and a plan to develop weaponized drones for use by the terror group.

[2] "shell companies" are companies that are incorporated but which have no independent operations, significant assets, ongoing business activities, or employees.

Source: FBI

1.5 The use of non-profit organisations in Terrorist Financing

Although the non-profit organisation sector, such as charities, are providing innumerable services to millions of people, they have been abused by terrorist organisations through a variety of means, posing as legitimate entities.

The abuse of charities for terrorist purposes is not limited to one form. This may include the exploitation of charity funding, abuse of charity assets, misuse a charity name and status and the setting up of a charity for an illegal or improper purpose.

The trustee of the charity always has a duty to be vigilant as risks of terrorism exist from the point where funds are raised and donations received, to the provision of services and other charitable activity.

Firms need to take appropriate measures to prevent a terrorist act in terrorist financing cases by educating their staff in order to identify possible indicators that suggests a risk of abuse of a charity that is related to a terrorist activity.

2. Money Laundering and Terrorist Financing

2.1 Similarities between money laundering and terrorist financing

Although money laundering and terrorist financing are two different crimes, they are often mentioned in the same breath. The reason for that is that both types of crimes are using similar methods to disguise the link between the criminal and the funding sources.

Terrorist organisations may require significant funding and employ modern techniques to manage and transfer funds between jurisdictions, hence the similarities with money laundering.

Additionally, both crimes keep an eye on the AML deficiencies of a countries controls to decide how and where to move their funds so as to avoid detection and possible investigation.

2.2 Differences between money laundering and terrorist financing

There are, however, key differences between terrorist financing and money laundering activities:

- The origin of funds: Although many terrorists fund their activities through the proceeds of crime, a great deal of terrorist financing comes from legitimate channels. When terrorist activities are funded by legitimate funds (i.e., funds donated by sympathizers or allies) it is difficult to identify the point when the funds become "terrorist funds".
- Amounts involved: Often, only small sums of money are required to commit terrorist acts, making identification, and tracking more difficult.

- Motivation: terrorists are committing their illegal acts because of their ideological beliefs where money launderers aim to gain more profit.
- Money trail: Persons who fund terrorist attacks and other activities are in many cases unrelated to the initiator where in money laundering, funds end up with the person(s) who initiated the proceedings.

Terrorist groups are known to have well-established links with criminal activity, and so there is often an overlap with money laundering. However, the methods needed to combat terrorist financing are quite different from those needed to combat money laundering. This is partly because, in many cases, terrorism can be funded by legitimate funds which mean it is not always easy for the firm to assess at what stage funds become terrorist assets.

Non-profit organisations, such as charities, can be particularly vulnerable to terrorist financing, and countries need to ensure that such organisations cannot be misused by terrorist groups posing as legitimate entities.

Whilst firms typically rely on the same internal policies and procedures to address money laundering and terrorist financing, the distinctive characteristics of terrorist financing make it particularly challenging to identify.

Case Study

In July 2015, Europol supported the Spanish Guardia Civil to dismantle a large Chinese money laundering network operating in Southern Europe. Over a six-year period, the network imported counterfeit products into Europe.

The imported products were sold to European Countries without declaring excise taxes. The undeclared profits were laundered using a large number of low-level associates, who deposited small sums of money in hundreds of personal bank accounts and transferred the money back to China.

The criminal network facilitated its activities by establishing complex corporate structures and relying on front men and third parties in their transactions. The network also offered money laundering and international remittance service to other organised crime groups in exchange for the payment of a negotiated percentage of the laundered funds. The group also operated several clothing factories in Madrid.

Predicate Offence: Counterfeit goods sales, tax evasion

Money Laundering through:

- Use low-level associates (smurfs)
- Use of complex corporate structures
- Assisting other crime groups to launder their activities.

Source: Europol

2.3 Criminalisation of money laundering and other offences

In most AML regulations, there are two broad categories of offences:

- Laundering Offences and
- Predicate Offences

Money Laundering Offence

While the specific rules and regulations in relation to money laundering differ from country to country, there are common features in the types of offences and regulatory obligations placed on financial services firms. The punishable criminal money laundering offences are:

- The conversion or transfer of property, knowing that such property is derived from criminal activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such an activity to evade the legal consequences of that person's action.

  This offence is committed by the person being investigated in relation to the proceeds of either; their own criminal activity or, that of someone else.

- The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of, property, knowing that such property is derived from criminal activity.
  - Examples include:
    - ✓ A lawyer who knowingly helps a person buy a house with criminal money
    - ✓ A person who arranges for their partner or parent to put a vehicle which is criminal property in their name.

- The acquisition, possession or use of property, knowing at the time of receipt, that such property was derived from criminal activity.

In all three cases above, we see the phrase "knowing that it is derived from criminal activity". Both, the FATF 40 recommendations and the 4th AML directive state that the "intent and knowledge required to prove the offence of money laundering may be inferred from objective factual circumstances". Some jurisdictions also use the principle "wilful blindness" which is the avoidance of knowledge of the facts or ignoring obvious money laundering red flags and is equivalent of actual knowledge of the illegal proceeds or the intention of a customer in a money laundering transaction.

As a result, a person can be prosecuted for a money laundering offence while he knows or ought to have known that any kind of property constitutes proceeds from the commission of illegal activities.

- **Failure to Disclose**

Additionally, a person who knows or reasonably suspects that another person is engaged in laundering or financing of terrorism offences, and the information, comes to his attention in

the course of his/her trade, profession, business, or employment, is obligated to disclose the said information to the Financial Intelligence Unit (FIU) as soon as it is reasonably practicable after it comes to his attention.

It constitutes a defence for the accused person if he proves that he intended to disclose to the FIU his suspicion or belief, or the facts on which he bases his suspicion or belief, in respect of the agreement or arrangement and that his failure to do so was based on reasonable grounds.

- **Tipping-Off**

'Tipping-off' in general terms can be explained as a disclosure of a secret warning or piece of secret information. In the context of money laundering, it is regarded as a situation where any individual discloses information that could affect the investigation or pervert the course of justice.

'Tipping-off' also contains a separate offence of prejudicing an investigation by:

- alerting individuals to an investigation being, or about to be undertaken
- destroying, concealing, or falsifying relevant documents

The firm cannot, at the time, tell a customer that a transaction is being delayed because the law enforcement authority is investigating, and a report is awaiting consent from FIU. This cannot be disclosed even later, unless law enforcement agrees, or a court order is obtained permitting disclosure.

This is clearly stated in FATF recommendation 21 which outlines that "financial institutions, their directors, officers and employees should be prohibited by law from disclosing the fact that a suspicious transaction report (STR) or related information is being filed with the FIU". A risk exists that customers could be unintentionally tipped off when the obliged entity is seeking to perform its CDD obligations in these circumstances. Obliged entities should take into account the risk of tipping-off when performing the CDD process. If the institution reasonably believes that performing the CDD process will tip-off the customer, it may choose not to pursue that process, and should file a suspicious transaction report to the FIU.

There might be cases where the customer wants to exercise his "right of access" under GDPR (General Data Protection Regulation) or any other data protection regulation. This means that normally an obliged entity would be obligated to provide the customer with information regarding the purposes of processing his personal data, the recipients of the customer's personal data, the duration of storage etc. However, under anti-money laundering regulations, the customer's "right of access" may be wholly or partially waived for the purposes of proper fulfilment of the anti-money laundering obligations of obliged entities and to avoid obstruction of anti-money laundering investigations. In this respect, employees are not allowed to disclose to the customers that want to exercise their "right of access" under GDPR, that there is a money laundering investigation with regards to him or her.

To reduce the risk of an employee "tipping-off" it is best practice for the MLCO to provide guidance to anyone making a report of suspicious activity. Such guidance could cover what can and cannot be said and how to respond to client queries.

- **Aiding and Abetting, Inciting and Attempting**

Aiding, abetting means that anyone trying to help money launderers is also committing a money laundering offence. It also includes anyone who is inciting money laundering. Most regulations, include measures to ensure that aiding and abetting, inciting, and attempting an offence is publishable as a criminal offence.

Predicate offences

Predicate offences are:

- all criminal offences punishable with imprisonment exceeding one year, as a result of which proceeds have been derived which may constitute the subject of a money laundering offence
- financing of terrorism offences as well as the collection of funds for the financing of persons or organisations associated with terrorism
- drug trafficking offences
- all offences, including tax crimes related to direct taxes and indirect taxes, which are punishable by deprivation of liberty or a detention order for a maximum penalty of more than one year.

In the context of financial services, this would cover any crime that generates proceeds.

Each country has its own range of predicate offences and it can decide, according to its domestic law, how it will define these offences and the nature of various elements that will constitute them as serious offences. The FATF has issued a designated list of offences that countries can use to decide on the range of offences to be covered as predicate offences. The list includes:

- participation in an organised criminal group and racketeering
- terrorism, including terrorist financing
- trafficking in human beings and migrant smuggling
- sexual exploitation, including sexual exploitation of children
- illicit trafficking in narcotic drugs and psychotropic substances
- illicit arms trafficking
- illicit trafficking in stolen and other goods
- corruption and bribery
- fraud
- counterfeiting currency
- counterfeiting and piracy or products
- environment crime
- murder, grievous bodily injury
- kidnapping, illegal restraint and hostage-taking
- robbery or theft
- smuggling (including in relation to customs and excise duties and taxes
- tax crimes (related to direct and indirect taxes)
- extortion
- forgery
- piracy and
- insider trading and market manipulation.

In the EU, the definition of criminal activities which constitute predicate offences for money laundering was not uniform. This created loopholes to the criminalisation of predicate offences, especially in cases where a predicate offence in one Member State was not a predicate offence in another Member State. The 6th AML directive (see Chapter 2) harmonizes the definition of the predicate offence taking into consideration FATF's designated list of predicate offences and aims to close any loopholes between Member States national legislations. The 6th AML Directive also includes cybercrime in the list of predicate offences.

3. Learning summary

- Money laundering is the process by which criminals seek to conceal the true origins and/or ownership of the proceeds, or benefits of a criminal activity. It is usually performed in three stages: Placement, layering and integration.
- Money laundering has significant macroeconomic consequences including increased exposure to organised crime and corruption, undermining the legitimate private sector, weakening the financial sector, dampening effect on foreign investments, loss of control in decisions regarding economic policy, economic instability and diminishing government tax revenues.
- Terrorist financing and money laundering are generally using the same methods to hide the proceeds of their crimes.
- Money laundering and terrorist financing differ in the origin of funds, the motives of the criminals, the amounts involved and the money trail.
- Money laundering offences include 1. conversion, transfer of property, 2. concealment or disguise of true nature, source location, disposition, movement, rights with respect to, or ownership of property, and 3. the acquisition, possession or use of property knowing that such property is derived from criminal activity. Failure to disclose and tipping off are also money laundering offences.
- A predicate offence is a serious crime that generates proceeds.

4. End of Chapter Questions

Think of an answer for each question and refer to the chapter content for confirmation.

- ✓ What is money laundering?
- ✓ What are the macroeconomic consequences of money laundering and terrorist financing?
- ✓ Give examples of the three stages of money laundering
- ✓ What is financing of terrorism?
- ✓ What are the similarities between money laundering and terrorist financing?
- ✓ What are the differences between money laundering and terrorist financing?
- ✓ What are the main types of money laundering and predicate offences?

NOTES

Chapter 2

AML Supervision

Learning Objectives

- Learn about the international bodies affecting the anti-money laundering regulatory environment (FATF, European Commission, MONEYVAL, The Basel Committee, The Wolfsberg Group)
- Learn about the FATF 40 Recommendations.
- Learn about the main provisions of the European 4th, 5th and 6th AML Directives.

Introduction

Supervisors around the world are trying to develop practices and standards on a national basis, that will be in line with international standards with regards to money laundering and terrorist financing. The purpose is to safeguard the integrity of the financial and non-financial system and avoid potential violation of the global international anti-money laundering standards. Supervisors also need to cooperate with each other to combat money laundering and terrorist financing and in many cases, this can be challenging.

The FATF and other standard-setting bodies, such as Basel and the European Commission, require that financial institutions and other obliged entities must take specific measures to combat money laundering and terrorist financing and are required to comply with KYC and CDD requirements, including those firms that have operations in more than one jurisdiction.

These bodies, issue standards that are accepted globally and provide guidance to the financial and non-financial sector on how to mitigate their money laundering risk and avoid negative consequences of being involved in money laundering or terrorist financing. They also oblige financial institutions and certain other service providers, to establish anti-money laundering procedures and train their staff in relation to them.

In this course, we will understand the role of the FATF as an International Standard setting body with regards to money laundering and terrorist financing. We will then look into two European bodies, the European Commission and MONEYVAL. We will also understand the role of the Basel Committee that sets AML standards for banks and Wolfsberg Group for the whole financial sector.

1. Bodies to Combat Money Laundering and Terrorist Financing

1.1 The FATF

The FATF was established in Paris in 1989 by the "Group of Seven" as an inter-governmental body, the mission of the FATF was to set international standards to foster the establishment of national and global measures to combat money laundering. In 2001, the development of standards against terrorist financing was added to the mission of the FATF.

The objectives of the Financial Action Task Force (FATF) are to set standards and promote effective implementation of legal and operational measures for combatting money laundering, terrorist financing and other related threats to the integrity of the international financial system. The FATF aims to ensure a coordinated global response to organised crime, corruption, and terrorism.

The FATF develops annual typology reports showcasing current money laundering and terrorist financing trends and methods. It also conducts peer reviews of each of its members on an ongoing basis to assess levels of implementation of the FATF Recommendations, providing an in-depth description and analysis of each country's system for preventing criminal abuse of the financial system.

DID YOU KNOW?

As of 2020, the FATF had 39 members - 37 countries and 2 organisations (European Commission and Gulf Cooperation Council). It has also established four regional groups, known as the International Co-operation Review Group, which represent the Americas, Asia Pacific, Europe and the Middle East and Africa.

Using input from its regional groups, it has undertaken an exercise to identify countries with inadequate AML measures, originally referred to as Non-Co-operative Countries and Territories (NCCT).

FATF issues two public documents three times a year:

- the FATF Public Statement which identifies jurisdictions that have strategic AML/CFT deficiencies, distinguishing between those jurisdictions which have applicable countermeasures and those that do not have countermeasures and have not made sufficient progress to address their deficiencies and

- "Improving Global AML/CFT Compliance Ongoing Process" which identifies jurisdictions that have deficiencies but have a high-level political commitment to address them.

1.2 EUROPEAN COMMISSION

The European Commission is the European Union's executive body and represents the interests of Europe as a whole. It drafts proposals for new European laws and manages the implementation of European Union's policies.

It is one of the two organisations - members of the FATF and it sets out a series of measures designed to strengthen the EU's framework to fight against money laundering and terrorist financing and close any loopholes or weak links in the EU's Member States anti-money laundering rules.

The Commission closely monitors the practical implementation of the 4th, 5th and 6th AML Directives in the EU member states.

It also adopts delegated regulations in relation to third countries which have strategic deficiencies in their money laundering and terrorist financing regimes and pose significant threats to the financial system of the Union. It issues and regularly updates a list of high risk third countries with strategic deficiencies that obliged entities throughout the EU need to take into consideration when assessing their customers in relation to the money laundering and terrorist financing risks. In 2020, it has issued a revised methodology of assessing high-risk third countries to ensure that the updated EU high-risk third country list is in line with the FATF list.

1.3 MONEYVAL

The Committee of Experts of on the Evaluation of AML measures and the financing of terrorist, MONEYVAL, is a permanent body of the Council of Europe, entrusted with the task of assessing compliance of its members with FATF's 40 Recommendations. MONEYVAL evaluates compliance of jurisdictions which are members of the EU and are not members of the FATF but also members of the EU that are members of the FATF but request to continue to be evaluated by MONEYVAL.

MONEYVAL was established in 1997 and its objectives are to ensure that its members have in place effective systems against money laundering. Its tasks include to:

- assess its members' compliance with all relevant international standards such as the FATF Recommendations, and the effectiveness of their implementation through a peer review process of mutual evaluations,

- formulate recommendations to improve the effectiveness of its members' national AML regimes to combat money laundering and terrorist financing and their capacities to co-operate internationally in these areas,
- conduct thematic typologies research of money laundering and terrorist financing methods, trends and techniques and issue reports,
- conduct other research into issues relating to money laundering and the financing of terrorism,
- undertake activities to raise awareness of major global policies and operational initiatives to counter money laundering and the financing of terrorism,
- after consultation with the European Committee on Crime Problems (CDPC), proposes recommendations for adoption by the Committee of Ministers which would improve the international fight against money laundering and the financing of terrorism,
- contributes actively to the global fight against money laundering and the financing of terrorism by working closely with other key international partners, including the FATF, the IMF, the World Bank, the United Nations, the European Union and other FATF-Style Regional Bodies (FSRBs) in the global network of AML/CFT assessment bodies.

1.4 The BASEL Committee

It was established in 1974 and its mission is to serve central banks in their pursuit of monetary and financial stability, to foster international cooperation in those areas and to act as a bank for central banks.

It introduces and revises guidelines for banks to strengthen the interaction and cooperation between prudential and money laundering and terrorist financing supervisors. The guidelines are consistent with the goals and objectives of the standards of the FATF.

It also issues and updates the Basel Framework, which is the full set of standards of the Basel Committee on Banking Supervision, which is the primary global standard setter for the prudential regulation of banks.

The Basel Committee provides guidance as to minimum standards for worldwide implementation for all banks. These standards may need to be supplemented and/or strengthened, by additional measures tailored to the risks of particular institutions and risks in the banking system of individual countries. For example, enhanced diligence is required in the case of higher-risk accounts or for banks that specifically aim to attract high net-worth customers.

1.5 The Wolfsberg Group

The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to anti-money laundering and counter terrorist financing policies.

In 2000, Wolfsberg group has issued the Wolfsberg Anti-Money Laundering (AML) Principles for Private Banking. The specific guidelines were revised in 2002 and in 2012. Since then, the Group has published a significant number of documents with regards to money laundering and terrorist financing such as principles, guidance, statements, and Frequently Asked Questions (FAQ).

Materials published by the Wolfsberg Group are designed to provide all financial institutions with guidance on financial crime risk management.

1.6 The Egmont Group

The Egmont Group was created in 1995 from a number of national Financial Intelligence Units (FIUs) that were seeking cooperation among them. Today it includes more than 150 FIRs. It is an international network designed to improve interaction amongst FIU in the areas of communication, information sharing, and training. The goal is to provide a forum for FIUs around the world to improve support to the national governments in the fight against money laundering, terrorist financing and other financial crimes.

2. Global AML Standards

2.1 The FATF 40 recommendations

In April 1990, the FATF has issued a report containing a set of 40 Recommendations which were intended to provide a comprehensive plan of action needed to fight against money laundering. In October 2001 when terrorist financing was brought under its scope, it issued "Eight Special Recommendations" to deal with the issue of terrorist financing. In October 2004, the FATF published a "Ninth Special Recommendation", and this resulted to the 40+9 Recommendations.

In February 2012, the FATF completed an extensive review and wide consultation and the recommendations were re-issued. The revised recommendations deal with new threats such as the proliferation of weapons of mass destruction and requires countries to be clearer on transparency and tougher on corruption. The 9 Special Recommendations on terrorist financing were now fully integrated into the revised set of 40 recommendations against money laundering.

The FATF recommendations are globally accepted and recognized as the international standards for combatting money laundering and terrorist financing and the proliferation of weapons of mass destruction.

Although the FATF is a "policy-making" body and its recommendations do not have the force of a law, they play an important role in the development of national legislations by most countries. The FATF 40 Recommendations provide governments and other supervisory bodies with stronger tools to act against financial crime. The regulations implemented at a national level often contain additional requirements with regards to money laundering and terrorist financing to address the risks in the specific jurisdiction.

The key aspects of the FATF Recommendations are:

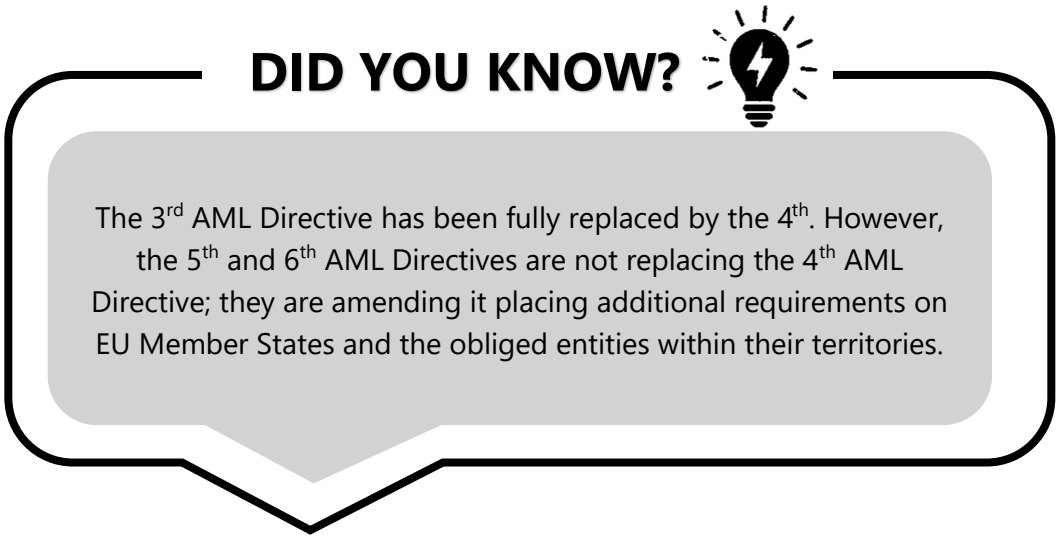
- place emphasis on the risk-based approach to money laundering and terrorist financing.
- focus on ultimate beneficial ownership of companies and other entities.
- Recognize international sanctions and counter-proliferation measures as global standards.
- Provide a revised definition of PEPs (Politically Exposed Persons) to include domestic PEPs (the previous definition only included foreign PEPs[3]).
- Inclusion of tax crimes as predicate offences of money laundering.
- Prevention of abuse of non-profit organisations.

[3] Foreign PEPs are individuals who are or have been entrusted with prominent public functions by another country, for example Heads of state or Heads of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

2.2 The European Directives

Despite the substantial progress made in the implementation of the anti-money laundering measures in the EU, illegal funds still exist and harm the integrity of the financial markets. Money laundering, terrorist financing and organised crime are significant problems in the EU. Efforts on a national level are not enough to combat money laundering and terrorist financing. Cooperation between EU member states and the European Union as a whole is appropriate.

The EU is closely considering the prevention of Money Laundering and is developing significant direction to its member states to effectively set anti-money laundering measures within their territories. Up to 2020, the EU has issued 6 anti-money laundering directives each time requiring member states to transpose it to their national legislations.


DID YOU KNOW?
The 3rd AML Directive has been fully replaced by the 4th. However, the 5th and 6th AML Directives are not replacing the 4th AML Directive; they are amending it placing additional requirements on EU Member States and the obliged entities within their territories.

2.3 The 4th AML directive

The 4th AML Directive (2015/849) was approved in 2015 and its purpose was to strengthen and align the AML regime in the EU with the FATF recommendations. It also expands its scope to several other entities that were not regulated back then, such as lawyers, accountants, the gambling sector, and services like trading of goods more than €10.000 in cash. This means that more firms are required to comply with the requirements of the directive. All EU Member States have transposed the specific directive into their national legislation. It mainly imposes obligations to the firms to:

- Use a risk-based approach when assessing their money laundering and terrorist financing risks
- Verify the identity of clients through customer due diligence (CDD) requirements
- Establish effective monitoring of customers' transactions and activities
- Maintain systems of internal and external reporting of suspicious transactions.
- Establish and implement internal controls to meet their obligations.

- Keep records of the customers' data and transactions

Strengthening the application of the Risk-based approach

The 4th AML Directive focuses on the application of the Risk-based Approach. This means that obliged entities within the EU need to determine the level of money laundering and terrorist financing risk posed by a client relationship in advance and conduct regular monitoring of transactions according to this risk. Each individual business relationship must be approached according to the money laundering and terrorist financing risks posed to the obliged entity by the specific business relationship.

Obliged entities are required to identify and assess their risks considering factors such as customers, countries or geographic areas, products, services and transactions and delivery channels. These risk assessments must be up-to-date and me made available to competent authorities if required.

Senior Management definition

According to the directive, a "senior manager" is "an officer or employee with sufficient knowledge of the institution's money laundering and terrorist financing risk exposure and sufficient seniority to take decisions affecting its risk exposure, and need not, in all cases, be a member of the board of directors". According to this definition, the Compliance Officer appointed in an obliged entity must be a member of the "Senior Management".

Definition of Obliged Entities

The Directive applies to:

- credit institutions
- financial institutions (which includes money service businesses)
- the following natural or legal persons when carrying out their professional activities (designated non-financial businesses and professions – DNFBPs)
  - ✓ auditors, external accountants, and tax advisors
  - ✓ notaries and other independent legal professionals that act on behalf of and for their client in any financial or real estate transaction, or by assisting in the planning or carrying out of transactions for their client concerning the:
    - buying and selling of real property or business entities
    - managing of client money, securities or other assets
    - opening or management of bank, savings or securities accounts
    - organisation of contributions necessary for the creation, operation or management of companies
    - creation, operation or management of trusts, companies, foundations, or similar structures
  - ✓ trust or company service providers
  - ✓ estate agents
  - ✓ other persons trading in goods through payments that are made or received in cash amounting to EUR 10,000 or more - whether the transaction is carried out in a single operation or several operations that appear to be linked
  - ✓ providers of gambling services

DNFBPs are obliged to report to the relevant FIU a suspicious transaction when providing legal advice for the creation, operation of businesses but also when they are engaged in financial or real estate transactions such as buying or selling real estate property, managing client assets, opening or management of a bank account, organisation for the creating or management of companies, etc. Under the 3rd AML Directive, these professionals used to consider all activities as privileged information and as a result they did not report any suspicious transactions to the FIU. The 4th AML Directive clarifies that they are not when they involve information with regards to a predicate or money laundering offence.

The 4th Directive applies to the entire gambling sector, while the 3rd AML Directive was only applied to the casinos.

Definition of the Beneficial Owner of a Legal Person

Obliged entities are required identify any person who owns or controls more than 25% of the shares or has an ownership interest of more than 25% in an entity, including bearer shareholders. However, if no controlling shareholder is found, then a senior manager may be considered as the beneficial owner of the client and needs to be sufficiently identified and verified. This is really

DID YOU KNOW?

A bearer share is a normal share in a company but that the name of the owner is not recorded on the physical certificate or in a public register. The name of the owner is simply listed as "The Bearer". The owner of the bearer share is the physical holder of the certificate. In many national regulations, its use is prohibited.

The 4th Directive also requires EU Member States to take appropriate measures to prevent misuse of bearer shares by requiring obliged entities to take measures and identify the owners of the bearer shares.

Creation of Beneficial Ownership Information Registries

The directive requires Member States to ensure that obliged entities obtain and retain information about the beneficial owners of their clients, including details of this ownership. This information will be included in a central beneficiary ownership registry that will be accessible to Competent Authorities, FIUs and other governmental authorities as part of their role in money laundering and terrorist financing investigations. These authorities will have a timely and unrestricted access. The register will also be available to regulated entities for their KYC and CDD obligation but also to any other person that can demonstrate a legitimate interest.

An exception to the above registration can be given to owners, when there is a risk of fraud, blackmailing, kidnapping, or of any other criminal action against the named beneficial owners. However, the reasoning must be adequately detailed, and, no exemption will be given to financial or credit institutions.

Creation of trust registry

Trustees of express trusts are also required to obtain and hold adequate, accurate and current information about the trust's settlor, trustees, protector, and beneficiaries or classes of beneficiaries and to make this information available to regulated entities.

In the case of **Trusts**, the definition of beneficial owner includes the settlor, the trustee, the protector, the beneficiaries or the class of beneficiaries and any other natural person exercising ultimate control over the trust directly or indirectly. This information will be held in a central trust registry.

Politically Exposed Persons (PEPs)

Following the FATF's recommendations, the 4th Directive provides a uniform definition of Politically Exposed Persons within the EU and broadens the PEP definition so as to include domestic PEPs. It also specifies that, when an obliged entity is dealing with a PEP, Enhanced Due Diligence (EDD) should always be carried out. The definition of a PEP that applies to all EU Member States is:

- A natural person who is or who has been entrusted with prominent public functions and includes the following:
    a. heads of State, heads of government, ministers and deputy or assistant ministers
    b. members of parliament or of similar legislative bodies
    c. members of the governing bodies of political parties
    d. members of supreme courts, of constitutional courts or of other high-level judicial bodies, the decisions of which are not subject to further appeal, except in exceptional circumstances
    e. members of courts of auditors or of the boards of central banks
    f. ambassadors, chargés d'affaires and high-ranking officers in the armed forces
    g. members of the administrative, management or supervisory bodies of State-owned enterprises
    h. directors, deputy directors and members of the board or equivalent function of an international organisation.

No public function referred to in points (a) to (h) shall be understood as covering middle-ranking or more junior officials.

- 'family members' include:
    a. the spouse, or a person considered to be equivalent to a spouse, of a politically exposed person
    b. the children and their spouses, or persons considered to be equivalent to a spouse, of a politically exposed person
    c. the parents of a politically exposed person

- 'persons known to be close associates' means:
    a. natural persons who are known to have joint beneficial ownership of legal entities or legal arrangements, or any other close business relations, with a politically exposed person
    b. natural persons who have sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the de facto benefit of a politically exposed person.

Penalties

Penalties under the 4th AML Directive are even stricter, especially for credit and financial institutions. Legal persons may receive a maximum fine of €5 million or 10% of total annual turnover. Natural persons may also receive a maximum fine of €5 million.

It also sets out a framework for breaches in the areas of due diligence, suspicious transactions reporting, record keeping and internal controls.

New cooperation regime for Financial Intelligence Units (FIUs)

Following the FATF Recommendations, the 4th AML Directive require countries to establish an autonomous and operationally independent FIUs within their territories, that will receive and analyse suspicious transaction reports provided by obliged entities and other information relevant to money laundering, associated predicate offences and terrorist financing. In the UK, the FIU is the National Crime Agency or NCA.

The 4th AML directive also aims to strengthen the role of the FIUs and their international cooperation efforts especially in respect of exchanging of information with other FIUs. It addresses the role of the FIU and requires Member States to ensure that the FIUs cooperate with each other to the best extent possible. Also, the FIU must be "provided with adequate financial, human and technical resources in order to fulfil its tasks".

FIUs from the various Member States should have close cooperation and exchange information. Local FIUs have the right to refuse data exchange only if this is against their local laws.

In the US the general requirements for reporting are not that different from the EU. After all, they both follow FATF's recommendations.

Reporting Obligations for suspicious transactions

Regulated entities should fill in relative reports for their FIUs when they have money laundering suspicions. They also need to respond to request by the FIU for additional information if necessary.

The above reporting obligations do not apply to notaries, independent legal professionals, tax advisors and accountants when they are assessing the position of their clients, when they are defending, of representing them in judicial proceedings.

Obliged entities should not execute transactions where there is suspicion for money laundering, unless they believe that the non-execution will hinder the efforts to detect the beneficiaries of these transactions. In that case, they may execute but inform their respective FIU immediately afterwards. But in most cases, obliged entities must not continue or complete a transaction until they receive further guidance from the FIU.

It is strictly forbidden to alert a customer that information about his activities has been given to the FIU. This is the so-called "tipping-off" and it constitutes an offence.

Data Protection and Record Keeping

The Directive has in place a specific record keeping obligation for the obliged entities. KYC documents, as well as other documentation related to the execution of a transaction, should be retained for a 5-year period from the end of the business relationship with their customer.

The directive also requires obliged entities to delete the relevant data after the five-year period elapses, unless there is pending investigation. In this case, they are allowed to retain the data for a maximum period of another 5 years.

Policies, Procedures and Supervision

Regarding Policies, Procedures and Supervision, the Directive requires obliged entities which are part of a Group, should apply group-wide policies. Where a company operates in other EU Member States, the competent authority of the home Member State should be responsible for supervising the obliged entity's application of group-wide AML/CFT policies and procedures.

Obliged entities established in the Union which are located in high-risk third countries, where those branches or majority-owned subsidiaries fully comply with the group-wide policies and procedures need to ensure that they apply the group-wide AML policies and procedures. When a company operates in a third country, where local laws do not allow the implementation of provisions of the Directive, it must take additional measures to effectively manage the risks created.

Obliged entities should take measures proportional to the risks they face, their staff should be aware of these risks and the measures taken are pursuant to the Directive.

All policies, procedures and AML controls need to be proportionate to the risk faced by the obliged entities. All employees must be aware of the entity's risks but also be aware of the measures taken to mitigate these risks.

Minimisation of the use of anonymous e-money products

Under the 4th AML Directive, anonymous electronic money stored in pre-paid cards is limited to €250. The anonymous prepaid cards should be exclusively used for the purchase of goods or services, should only be loaded once, and should not be funded anonymously. Regulated Entities that issue this type of cards must carry out transaction monitoring to enable detection of suspicious transaction.

Holders of anonymous prepaid cards may redeem up to €100 per month. Higher value transactions require full identification of card holders.

2.4 The 5th AML Directive

While the implementation of the 4th AML Directive was in progress, the European Commission was working on the following amendments due to the rapid changes in the financial environment:

- Virtual currencies exchange platforms and wallet providers to become obliged entities.
- Eliminate further the types of electronic money products to be exempted from KYC and CDD.
- Cooperation between Member States competent authorities to be fostered.
- The enhanced due diligence measures for high risk third countries will be harmonized between EU member States.
- Access to beneficial ownership registries to be expanded.

The purpose of these amendments was to further reinforce EU rules for combating Money Laundering and to counter the financing of terrorist activities, but also to regulate certain modern financial activities that are becoming more popular and have remained so far outside the scope of EU rules and legislation.

The main changes include:

Beneficial Ownership Registers

In addition to the requirement of the 4th AML directive with regards to the creation of a beneficial ownership registers, the 5th AML Directive proposes that EU citizens are granted access to these registers without having to demonstrate "legitimate interest". The public use of the beneficial ownership register aims to promote transparency and prevents the usage of legal entities or arrangements for illicit purposes.

The access of the public to the beneficial ownership information should be permitted in a coordinated manner through clear and transparent rules. To protect the privacy of beneficial owners, Member States should be able to identify people who are asking access to the registry.

The disclosure of beneficial ownership information will enable third parties, and the society in general, to know who the UBOs are and thus, promote public scrutiny, the misuse of legal entities and corporate structures for illegal purposes.

Virtual Currencies and Custodian Wallet Providers

Providers of exchange services between virtual and fiat currencies and custodian wallet providers were outside the scope of AML regulations. As a result, money launderers and terrorists could use this type of services to transfer money within the EU while at the same

time maintaining their anonymity. Suspicious transactions made through virtual currencies were not sufficiently monitored by the authorities, which are unable to link the transactions to identified persons. In addition to that, it was stressed that virtual currencies entail a risk that they may be used by terrorist organisations to conceal financial transfers.

A wallet provider is an entity that provides a virtual currency wallet (i.e. a software application or other mechanism/medium) for holding, storing and transferring bitcoins or other virtual currency).

DID YOU KNOW?

A wallet holds the user's cryptographic private keys, which allow the user to spend virtual currency allocated to the virtual currency address in the block chain. A wallet provider facilitates participation in a virtual currency system by allowing users, exchangers, and merchants to conduct the virtual currency transactions more easily.

The 5th AML Directive brings virtual currency platforms and wallet providers into the scope, responding to the huge growth in the use of virtual currencies and Fintech in general.

Exchange service and wallet providers will have to be authorized and registered and, as a result, to implement necessary customer due diligence controls, monitor transactions and report any suspicious activity to the relevant national authorities, like any other financial institution. They also need to be able to associate the virtual currency address with the identity of the owner.

Consequently, the competent authorities will match all the bank and payment accounts with their corresponding account holders, proxy holders and beneficial owners. Therefore, anonymous or pseudonymous activities and persons, currently prevailing in the crypto field, will be diminished for purposes of AML rules.

Anonymous electronic money products

The 5th AML Directive lowers even further the transaction threshold for anonymous electronic money and prepaid card instruments from €250 to €150 and their monthly redemption limit is reduced to €50. Anonymous prepaid cards are widely used and, in most cases,, they are used for legitimate purposes. However, the 5th AML directive imposes a substantially low limit to prevent the use of this type of products for criminal purposes.

Broader Information Sharing

Under the 5th AML Directive, Financial Intelligence Units (FIUs) are given the authority to obtain the addresses and identities of owners of virtual currencies. The information exchange

between FIUs are to be improved as well as their access to law enforcement information necessary for the performance of their tasks.

These measures aim to speed up criminal investigations and enable authorities to combat cross-border crime more effectively.

DID YOU KNOW
While the 4th AML Directive focuses on the risk-based approach and the 5th AML Directive focuses on transparency, the 6th AML Directive focuses on criminalisation.

2.5 The 6th AML Directive

The 6th AML Directive aims to harmonize the definition of money laundering across the EU Member States, expand the number of offences that fall under the definition of money laundering and impose tougher punishments for those involved in money laundering. More specifically, the changes with regards to the previous directives include:

- Defining all 22 predicate money laundering offences
- Harmonizing the definition of money laundering across the EU
- Staff will need to be trained to recognize all predicate offences
- Aiding, abetting and attempting to commit money laundering will also be an offence
- Imposing a minimum four-year prison sentence for serious offences
- Extending criminal liability to legal persons

Laundering Offences

According to the 6th AML Directive, a party can be found guilty of money laundering if he intentionally is engaged in one or more of the following activities:

a. converts or transfers a property derived from a criminal activity for the purpose to conceal or disguise the illicit origin of the property or of assisting in this activity

b. conceals, disguise the true nature, location disposition, movement, rights with respect to, ownership of property,

c. acquires, possess or use this type of property

It is also considered a criminal offence when the offender suspected or ought to have known that the property was derived from criminal activity.

Predicate Offences

The European Union with the introduction of the 6th AML Directive provides a list of 22 predicate offences that constitute money laundering. All EU member states need to comply with the revised definition. These predicate offences are:

1. participation in an organised criminal group and racketeering
2. Terrorism including financing of terrorism
3. trafficking in human beings and migrant smuggling
4. sexual exploitation
5. illicit trafficking in narcotic drugs and psychotropic substances
6. illicit arms trafficking
7. illicit trafficking in stolen goods and other goods
8. Corruption and bribery
9. Fraud
10. counterfeiting of currency
11. counterfeiting and piracy of products
12. environmental crime
13. murder, grievous bodily injury
14. kidnapping, illegal restraint and hostage-taking
15. robbery or theft
16. Smuggling
17. tax crimes relating to direct and indirect taxes, as laid down in national law
18. Extortion
19. Forgery
20. Piracy
21. insider trading and market manipulation,
22. cybercrime

Regulated entities should ensure that they understand the risks arising from the new predicate offences and ensure that they have appropriate AML controls in place to protect themselves. They need to manage their resources in a way to enable them to identify possible criminal activity through the transaction monitoring and screening of customers. They also need to ensure that staff receives adequate training and that they understand the new risk environment.

3. Learning Summary

- The FATF has issued the 40 Recommendations which are globally recognized as the international standards to combatting money laundering, terrorist financing and other related threats to the integrity of the international financial system.
- The European Commission, Moneyval, Basel Committee and Wolfsberg Group are other international bodies that aim to assist in the implementation of the FATF recommendations
- The 4th AML Directive (2015/849) is in effect, replacing the 3rd Directive (2006/70/EEC). The main purpose of the 4th AML Directive is to strengthen the EU Anti-Money Laundering equipment and align the rules in the Union with the FATF recommendations.
- There have been amendments and changes in the following six areas: Introduction of the concept of the Risk Based Approach, Obligation to reveal beneficial owner information, Changes in the treatment of Politically Exposed Persons (PEPs), Changes

in policies and procedures, Changes in the penalties regime and Changes in the cash payments.

- The 5th Directive conveys virtual currency platforms and wallet providers into its scope. It also revises anonymous transaction limits on prepaid cards are reduced to €50, with higher value transactions requiring full identification of card holders.
- The 6th AML Directive aims to provide a harmonized definition of the "predicate offences" and "money laundering offences".

4. End of Chapter Questions

Think of an answer for each question and refer to the chapter content for confirmation.

- ✓ What is the role of the following with regards to the fight against money laundering?
  - The FATF
  - The European Commission
  - Moneyval
  - The Basel Committee
  - The Wolfsberg Group
  - The Egmont Group
- ✓ What are the FATF 40 recommendations?
- ✓ What are the main changes brought in the EU by:
  - The 4th AML directive
  - The 5th AML directive
  - The 6th AML directive

NOTES

Chapter 3

The AML Compliance Program

Learning Objectives

- Understand how governance plays huge role in the application of an anti-money laundering program.
- Understand the role of the Board of Directors, the Internal Auditor and the Compliance Officer.
- Learn the appropriate policies and procedures that need to be in place in every obliged entity.
- Know the importance of employees' education and training.

Introduction

The FATF recommendations form an important part of national AML regulations. Competent authorities in every jurisdiction need to establish anti-money laundering regulations and ensure that obliged entities within their territory comply with these regulations and that they have in place anti-money laundering measures and controls to prevent from being used from criminals for money laundering or terrorist financing purposes.

The effectiveness of an anti-money laundering and counter financing of terrorist (AML/CFT) program starts with the establishment of an anti-money laundering culture. The organisation's culture refers generally to the beliefs and behaviours of a company that determine how employees and the management interact and do business day-to-day. The importance of a positive corporate culture is highlighted by the growing number of corporate scandals relating to issues such as sanctions violations, financial misconduct, labour rigging and bribery and corruption.

A strong AML culture must be one with a strong commitment from the top and includes both, the managing of money laundering and terrorist financing risks and implementing integrated controls to meet compliance objectives. Developing an AML culture should not be done in isolation. AML/CFT controls should align with the organisation's broader risk appetite.

An anti-money laundering culture requires an appropriate anti-money laundering program that is generally made up of the following components:

Each of the elements that make up the framework play an important part to help firms detect and prevent criminals from misusing their products and services to launder the proceeds of crime. In general, regulators expect firms to design the controls that form this framework in a way that suits the nature, size and complexity of their business. This means that the controls used for a large global bank, for example, will likely be more complex than those used for a small insurance brokerage business.

An important theme that runs through all AML regulations is the use of a risk-based approach. This allows firms to both scale the controls they use to detect and prevent money laundering based on the size of their business and focus more resources on those areas where potential money laundering risks are assessed to be the greatest. The goal is to allow a firm to deal with money laundering risks in a proportionate way and allow firms to allocate their limited resources in areas where their money laundering and terrorist financing risks are higher.

1. Elements of a successful AML Compliance Program

1.1 The Board of Directors

The establishment of an anti-money laundering program of a regulated institution start and end with the responsibilities of the Board of Directors. They are responsible to embed a strong anti-money laundering compliance culture within the firm.

The Board of Directors or an equivalent body according to the type of business, is responsible to ensure that the firm has an AML compliance program in place and that it is working effectively. This includes:

- Understanding the types of financial crime risks to which their business could be exposed.
- Deciding the firm's risk appetite – or in other words, the types of customers or activities where the possible money laundering risks are so high the business cannot deal with those risks with the existing controls it uses as part of its AML compliance program.
- Overseeing the completion of a business-wide risk assessment. This assessment allows the business to determine the types of financial crime risks to which it could be exposed based on four main areas of risk – customers, jurisdiction or geography, products and services and channels of delivery.
- Raising awareness to the point that everyone, including the Board of Directors, Senior Management and all employees understand that the anti-money laundering compliance is not just one person's job, but everyone's responsibility.
- Appointing a Money Laundering Compliance Officer, Alternate Compliance and Assistants Compliance if necessary and that they have sufficient resources for the effective execution of their duties.
- Ensure that all employees are aware of the person who is appointed as a Money Laundering Compliance Officer and that there is in place a clear and quick procedure for the reporting of any suspicious activity.
- Determine the general policy principles of the firm for the prevention of money laundering and terrorist financing and communicates them to the AML Compliance Officer.
- Approving the risk management policies and procedures.
- Ensures that there are in place effective and enough systems and controls in place to comply with AML regulatory obligations.
- Assesses and approves the Money Laundering Compliance Officer Annual report and take appropriate actions to remedy possible weaknesses or deficiencies.

As an additional measure, regulated entities must designate an executive or non-executive member of the Board of Directors to be responsible for the implementation of the anti-money laundering standards and regulations by the obliged entity.

1.2 The Internal Audit Function

Where appropriate and, depending on the size and nature of a business, a successful independent internal audit must be established. The internal audit function reviews and evaluates, at least on an annual basis the appropriateness, effectiveness and adequacy of the policy, practices, measures, procedures and control mechanisms applied for the prevention of money laundering and terrorist financing.

The results of the audit will help the Board of Directors to ensure that the policies, procedures, and controls of the Obliged Entity remain up-to-date and will enable it to identify and manage deficiencies in the effectiveness of the organisation's AML program.

The internal auditor must be sufficiently qualified to ensure that his findings and conclusions are reliable. The findings and observations of the internal auditor are recorded in the Annual

Internal Audit Report, which is submitted to the Board of Directors which decides for the necessary measures that need to be taken to rectify possible weaknesses and deficiencies detected.

1.3 The Money Laundering Compliance Officer (MLCO)

One of the responsibilities of the Board of Directors is to appoint a Money Laundering Compliance Officer (MLCO), otherwise known as the Money Laundering Reporting Officer (MLRO). The Board of Director must also appoint an alternate compliance officer to replace him when he is absent and assistant compliance officers if necessary, taking into consideration the size and complexity of the organisation.

The MLCO must be a member of the senior management and is responsible for the implementation of the AML program within all lines of the organisation. In most jurisdictions, the appointment of the MLCO must be approved by the relevant supervisory authority. His responsibilities are outlined in the national AML regulations and may vary from country to country. Amongst others, his duties include:

With regards to **policies and procedures**:

- Design of appropriate policies, procedures, and controls for the prevention of money laundering and terrorist financing.
- Establishes the customers' acceptance policy.
- Prepares the AML manual of the organisation.
- Monitors the implementation and effectiveness of the policies, procedures and controls as stated in the AML manual.
- Ensures the maintenance of CDD and transaction records for five years after the end of the customer relationship.
- Submit an annual report to the Board of directors with regards to the firm's compliance with the AML regulations, along with any recommendations for changes or improvements.

With regards to **employees and employees' training**:

- Provides guidance for corrective measures if he identifies shortcomings and/or weaknesses.
- Determine the training needs of the employees of the organisation and organises appropriate training sessions.
- Establishing and maintaining adequate arrangements, including records, for staff awareness and training.

With regards to **suspicious transactions**:

- Receives information from the employees on the Internal Suspicious Transactions / Activity Report (STR/SAR).

- Investigate and evaluates the information received on the STR/SARs, using all of the information available to them to establish whether or not they believe they may be well-founded
- Reports to the FIU any suspicious transactions or activities.
- In case he decides not report a suspicious activity or transaction to the FIU, he must explain the reasons for this decision on the Internal Evaluation Report.
- Remain the central point of contact with the FIU and law enforcement agencies in his country.

The MLCO must detect, record, and evaluate, at least on an annual basis, all risks arising from existing and new customers, new financial instruments and services and updates and amends the systems and procedures applied by the Obliged Entity. The annual evaluation is recorded in the Compliance Officer annual report which is assessed and approved by the Board of Directors.

1.4 Employees obligations, training, and ongoing awareness

Most people do not realize that training is an essential control in the detection and prevention of money laundering. The employees are the most effective defence against money laundering and terrorist financing and the criminals who might seek to abuse the services provided by a firm. Regular training will allow employees to understand the legal obligations imposed on both them personally and the regulated entity. It is also an opportunity for obliged entities to ensure that employees and the Board of Directors are aware of the money laundering and terrorist financing risks posed by their activities and the policies, controls, and procedures that the regulated entity has in place.

The MLCO has a responsibility to ensure all members of staff undergo periodic training to ensure that they are aware of the requirements of the anti-money laundering law, AML policies and data protection. The training must also enable them to recognize and report to the MLCO suspicious transactions, so that the firm meets all the requirements imposed by the Regulations and anti-money laundering rules.

With regards to training, certain roles, such as the MLCO, will require more specific training, to ensure that they have the skills and knowledge to fulfil their regulatory duties.

In general, firms are required to ensure that the Board, senior management, and staff receive tailored training for employees in different positions and different level of responsibilities. For example, new employees should receive different training than employees working in the entity for years. Training must ensure that they have a good understanding of money laundering risks to which the business could be exposed, its risk appetite and warning signs or red flags that might indicate possible money laundering.

Firms can determine on a risk-basis, the frequency with which they undertake regular training with existing staff to ensure that new trends, changes to procedures and identified emerging risks and made aware to them but in most regulations, it needs to be undertaken at least on an annual basis.

Training must include topics related to each target audience. Effective training may present real-life money laundering schemes, cases that have occurred at the firm or other firms within the industry including, how the pattern of activity was first detected, its impact on the firm and its ultimate resolution.

When setting up an employee training program, the Obliged Entity should consider:

- which employees require training;
- what is the content of the training provided; (e.g. legal framework, transactions monitoring, procedures for reporting suspicious transactions/ activities, typologies/case
  studies of suspicious activities etc.)
- what form the training will take;
- how often training should take place;
- how employees will be kept up-to-date with emerging risk factors for the regulated entity.

2. Establishing an acceptable risk policy

2.1 Client Acceptance Policy

Each obliged entity needs to establish a client's acceptance policy to perform an accurate and complete risk assessment when onboarding clients. The client acceptance policy sets out the criteria and determine the basis on which a regulated entity enters into business relationships with its customers.

The purpose is to ensure that an obliged entity is able to understand the customer, his financial activity, the money laundering and terrorist financing risks posed by the specific client and ensure that the entity is in a position to manage these risks effectively.

The policy establishes:

- The criteria for accepting new customers (legal persons and individuals)
- The procedures to verify the identification of individuals and companies that the obliged entity will enter into a business relationship.
- The factors considered to classify a client that pose a low, medium or a higher-than-average risk to a firm and a description of these types of customers.
- Customers that are not accepted by the obliged entity.
- The conditions for termination of a business relationship.

DID YOU KNOW?

The criteria for accepting new clients should be established on a risk-based approach and consider risk factors related to the customer, the countries or geographical areas where the customer has links, the product, service and transaction risks and delivery channel risks.

The client's acceptance policy will be driven by the firm's risk appetite established as a result of the business risk assessment it has performed. The policy needs to include procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the most basic account-opening requirements for a working individual with a small account balance. On the other hand, for example, enhanced due diligence would be essential for an individual with a high net worth whose source of funds is unclear since the risk in being involved in money laundering is higher.

It is important that the customer acceptance policy is not so restrictive that it results in a denial of access by the public to financial services, especially for people who are financially or socially disadvantaged.

2.2 Establishing appropriate policies and procedures

Policies, procedures, and controls should be designed to mitigate the identified AML/CFT risks and should take into account the applicable AML/CFT laws and regulations that the obliged entity must comply with. They should clearly indicate the risk appetite of the business — in other words, what risks the business is prepared to accept and those that it is not. Revenue interests should not compromise or override compliance functions beyond the risk appetite of the institution.

Policies and procedures outline and explain the measures and controls a business applies to detect and prevent it from being used for money laundering, terrorist financing and other financial crimes. The AML procedures, policies and controls are also necessary to protect the obliged entity's brand and reputation against money laundering and terrorist financing risks and ensure that the obliged entity is compliant with the whole AML/CFT framework. For this purpose, these procedures must be in line with the firm's business risk assessment and approved by the Board of Directors or the Senior Management. A regulated entity must be able to demonstrate to the competent authorities that it has appropriate anti-money laundering and procedures in place.

The principles beyond the internal practices, measures, procedures and controls related to the prevention of money laundering and terrorist financing are set by the Board of Directors. These procedures include KYC and CDD procedures, record keeping, monitoring of transactions and suspicious transaction reporting procedures. We will see in detail these procedures in MO

All procedures and policies must be documented and be communicated to the employees of the organisation. The design of specific policies and procedures need to take into consideration the size of the business to determine the type and extent of measures required.

Employees must receive appropriate training with regards to these procedures to ensure that they employees have a solid understanding of the policies and procedures of the organisation as well as the consequences for failing to comply with them.

3. Learning summary

- A successful anti-money laundering program starts and ends with the responsibilities of the Board of Directors.
- Obliged entities are required to have an independent internal audit in place to test the effectiveness of the anti-money laundering program.
- The MLCO is responsible for overseeing the anti-money laundering policies and procedures.
- Employees need to understand their legal obligations with regards to money laundering and terrorist financing and receive regular training in order to identify suspicious transactions.
- Appropriate policies and procedures need to be in place that will enable an obliged entity and its employees apply anti-money laundering measures and controls.

4. End of Chapter Questions

Think of an answer for each question and refer to the chapter content for confirmation.

- ✓ What are the elements of a successful AML compliance program?
- ✓ What is the role of the Board of Directors in AML?
- ✓ What are the duties of the internal audit function?
- ✓ What are the duties of the MLCO?
- ✓ What are the main elements of a successful training program?

NOTES

Chapter 4

The risk-based approach

Learning Objectives

- Understand the concept of the risk-based approach.
- Perform appropriate identification and assessment of money laundering risks.
- Learn the factors that need to be considered by an obliged entity when assessing the anti-money laundering risks posed by a business relationship.

Introduction

In today's fast-changing financial environment, governments and obliged entities are exposed to money laundering and terrorist financing risks. International organisations and regulators are aiming to impose stringent requirements to financial and non-financial institutions in their fight against ML/TF.

Prior to the introduction of a risk-based approach (RBA) to AML, banks and financial institutions would manage their compliance obligations using a 'checkbox' approach – that is, simply fulfilling a standardized list of AML requirements for each customer. The concept of risk-based AML was first implemented in 2007 by the Financial Action Task Force (FATF) and further codified in its 2012 updated 40 Recommendations.

FATF's recommendation of using a RBA in combatting money laundering and terrorist financing, requires a deeper understanding of what a risk is and how to use risk management. In the EU, the ESAs have issued "Risk factor guidelines" in accordance with the 4th AML directive to assist obliged entities to assess specific factors when conducting their business-wide risk assessments and their customer risk assessments.

The concept of the RBA shifts the focus of AML compliance from post-analysis of data to proactive judgment. Obliged entities must work on an ongoing basis to understand the money laundering threats they face and deploy commensurate measures to manage their risk exposure. A successful RBA implementation needs a deep understanding of the ML/TF threats and vulnerabilities.

A reasonably designed RBA is one by which institutions identify the criteria to measure potential money laundering risks. Identification of the money laundering risks of customers and transactions will allow institutions to determine and implement proportionate measures and controls to mitigate these risks. Risks for some customers may only become evident once the customer has begun transacting through the account, making monitoring of customer transactions a fundamental component of an RBA.

The majority of governments around the world believe that the RBA is more effective in the area of AML/CFT because it is more:

- Flexible—as money laundering and terrorist financing risks vary across jurisdictions, customers, products and delivery channels, and over time.
- Effective—as companies are better equipped than legislators to effectively assess and mitigate the particular money laundering and terrorist financing risks they face.
- Proportionate—because a risk-based approach promotes a common sense and intelligent approach to fighting money laundering and terrorist financing as opposed to a "check-the-box" approach. It also allows firms to minimize the adverse impact of anti-money laundering procedures on their low-risk customers.

In this Chapter we will examine the elements of the RBA, the effective application and the factors that need to be considered when assessing the money laundering and terrorist financing risks on a business level, but also when assessing individual business relationships.

1. Understanding risks

1.1 The EU Supranational Risk Assessment

The first recommendation of the FATF creates the basic obligation that:

'Countries should identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action, including designating an authority or mechanism to coordinate actions to assess risks, and apply resources, aimed at ensuring the risks are mitigated effectively."

According to this recommendation, FATF members are required to conduct a risk assessment within their territory. In the EU, the 4th AML Directive requires first the European Commission (which is a FATF member) to conduct a risk assessment of money laundering and terrorist financing risks affecting the EU internal market and risks relating to cross border activities. This assessment should be updated every two years. The results of the assessment should be included in a report, known as the Supranational risk assessment.

The report aims to provide a systematic analysis of the money laundering or terrorist financing risks of specific products and services within the EU. It focuses on vulnerabilities identified at EU level, both in terms of legal framework and in terms of effective implementation. The report is available to member states and to obliged entities, to help them understand their anti-money laundering risks they are exposed to, on a country level but also on a business level.

1.2 National Risk Assessments

The 4th AML directive also requires EU Member States to conduct a risk assessment on a national level taking into consideration the supranational risk assessment. The purpose is for

countries, to obtain an understanding of the ML/TF risks they are exposed to, and apply an RBA to ensure that they have in place measures to prevent or mitigate money laundering and terrorist financing that are commensurate with the risks identified.

The national risk assessment identifies the level of risk for each financial and non-financial sector in the member state (high, medium high, medium, medium low, low). Where countries identify higher risks, they should ensure that their AML/CFT regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain conditions.

The results of the National Risk Assessments are available to obliged entities within the specific territory, the European Commission and to the relevant European Supervisory Authority (ESA). The report will assist obliged entities to design their internal policies, controls and procedures to combat money laundering and terrorist financing and take appropriate measures to keep money laundering and terrorist financing risks at an acceptable level.

DID YOU KNOW?

The ESAs are the European Banking Authority (EBA), the European Securities and Market Authority (ESMA), European Insurance and Occupational Pensions Authority (EIOPA).

1.3 The importance of RBA

The RBA is central to the effective implementation of the FATF Recommendations adopted in 2012. A risk-based approach requires financial institutions to have systems and controls that are commensurate with the specific risks of money laundering and terrorist financing they face. Risk assessment is one of the most important steps in creating a good AML/CFT compliance program. As money laundering risks increase, stronger controls are necessary. However, all categories of risk—whether low, medium, or high - must be identified and mitigated by the application of relevant controls, such as verification of customer identity, customer due diligence policies, suspicious activity monitoring and economic sanctions screening.

The principle of the RBA is that a company's resources should be directed in accordance with priorities so that the greatest risks receive the highest attention. There are no universally accepted methodologies that prescribe the nature and extent of an RBA.

The RBA involves identifying and categorizing money laundering risks and establishing reasonable controls based on risks identified. Obliged Entities are expected to exercise reasonable business judgement with respect to their clients' risk assessment.

The RBA does not prohibit obliged entities from establishing business relationships with customers who have a high money laundering and terrorist financing risk, but it assists them to effectively identify and manage these risks and bring them to an acceptable level.

1.4 Application of the RBA

A risk-based approach involves specific measures and procedures such as:

a. Identifying and assessing the money laundering and terrorist financing risks emanating from clients, services, geographical areas, and delivery channels of operation of the Licensed Firm and its clients,
b. Documenting in the relevant manual, the policies, measures, procedures, and controls to ensure their uniform application across the obliged entity by persons specifically appointed for that purpose by the Board of Directors / sole director / sole practitioner,
c. Managing and mitigating the assessed risks by the application of appropriate and effective measures, procedures and controls,
d. Continuous monitoring and improvements in the effective operation of the policies, procedures, and controls.

The risk-based approach carries specific benefits and challenges are:

Benefits:

- Better management of ML/RF risks.
- Obliged Entities focus where the risks are higher.
- Flexibility to adapt to risks that change over time.

Challenges:

- Create appropriate procedures and identifying appropriate information to conduct a risk assessment.
- Cost of compliance with AML/regulations.
- Find capable staff, able to make reliable judgements.

1.5 Business-wide risk assessments

Business-wide risk assessments should help firms understand which areas of their business are exposed to money laundering and terrorist financing risk and where they should prioritize and invest their resources in the fight against money laundering and terrorist financing. Obliged entities also need to establish the risk appetite in terms of the level of AML/CFT risks it is

prepared to accept and the risk appetite must be clearly indicated in the policies and procedures of the organisation.

Obliged entities must identify and assess the money laundering and terrorist financing risk associated with the products and services they offer, the jurisdictions they operate in, the customers they attract and the transaction or delivery channels they use to service their customers.

Based on the assessments conducted, firms should have in place controls, policies and procedures that enable them to manage and mitigate the identified risks effectively. The assessment is not a one-off task. It needs to be reviewed and updated regularly, depending on how circumstances develop and how threats evolve.

As a result of this analysis, the financial institution should develop a thorough understanding of the inherent risks in its customer base, products, delivery channels and services offered (including proposed new services) and the jurisdictions within which it or its customers do business. This understanding should be based on operations, transactions and other internal information collected by the regulated entity, as well as external sources. In identifying all relevant money laundering and terrorist financing risks, all relevant information must be considered. This usually requires expert input from the business lines, risk management, compliance, and legal units together with advice from external experts where necessary.

There is a growing body of publicly available helpful guidance on money laundering and terrorist financing risk assessments that should be taken into consideration. Such guidance is regularly published by FATF, regional FATF-styled bodies, regulatory agencies, other institutions such as the United Nations Office on Drugs and Crime (UNODC), the International Monetary Fund (IMF), the World Bank, and jurisdiction-specific information, guidance, and advisories.

DID YOU KNOW?

Firms that do not offer complex products or services and that have limited, or no international exposure may not need an overly complex or sophisticated risk assessment.

1.6 Identification of ML risks on business relationships

Obliged entities must use the findings from their business-wide risk assessment to decide on the appropriate level and type of CDD that they will apply to individual business relationships and occasional transactions, according to the money laundering and terrorist financing risks posed as a result of entering into a business relationship or carrying out an occasional

transaction (a transaction not carried out as part of a business relationship i.e., not carried out through an account).

A risk assessment process should consist of two distinct but related steps:

- Identification of the money laundering/terrorist financing risk
- The assessment of the money laundering/terrorist financing risk

emanating from particular customers, products, services and geographical areas of operation of the regulated entity and its customers.

When identifying money laundering and terrorist financing risks associated with a business relationship or an occasional transaction, firms should consider relevant factors that include:

- who their customer is,
- the countries or areas where the customer operates,
- the product or services the customers require and
- the way the product or service is delivered to the customer (delivery channel).

Information about these risk factors should come from various sources, such as commercially available tools or databases that pool information from several sources. The type and number of sources that will be used for each customer must be determined on a risk-based approach. For this purpose, the MLCO must collect data, information and reports published by international organisations such as:

- **Financial Action Task Force (FATF):** An international body that is the global money laundering and terrorist financing watchdog. It sets inter-governmental standards aiming to prevent illegal activities that harm the society.
- **MONEYVAL:** The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism. Its task is to assess compliance with the principal international standards to counter money laundering and the financing of terrorism, the effectiveness of their implementation and it also makes recommendations to national authorities in respect of necessary improvements to their systems.
- **European Commission**: Carries out risk assessments in order to identify and respond to the money laundering and terrorist financing risks affecting the EU internal market (Supranational risk assessments). It also identifies high-risk third countries having strategic deficiencies in their regime on money laundering and terrorist financing.
- **IMOLIN (International Money Laundering Information Network):** An Internet-based network assisting governments, organisations and individuals in the fight against money laundering. It also includes a database on legislation and regulation throughout the world, an electronic library, and a calendar of events in the anti-money laundering field.
- **IMF (International Monetary Fund):** Amongst other tasks, the IMF has as one of its primary responsibilities to develop a worldwide standard for AML/CFT in cooperation with other international organisations such as the World Bank, the United Nations, FATF and other regional bodies.

- **Transparency International**: It is a global movement with the aim to end the injustice of corruption and promote transparency, accountability, and integrity at all levels and across all sectors of society.
- **Other sources of information**: From national law enforcement agencies, alerts, governments' national risk assessment and other reports issued by national and international standard-setting bodies.

1.7 Customer Risk Assessment

The risk-based approach allows a firm to approach each one of its customers based on the money laundering and terrorist financing risk they carry. Know Your Customer (KYC) information allows a firm to perform a risk assessment of all new customers. On a risk-based approach, a firm can assess the level of potential money laundering risk associated with a customer. It is then able to decide whether to accept that relationship or whether the money laundering / terrorist financing risk involved exceeds its risk appetite, and so declines the relationship.

Although KYC documents and initial CDD procedures are essential part of a firm's AML controls, these procedures must continue throughout the business relationship of the client with the obliged entity. The risk assessment of the customer needs to be performed on a regular basis to ensure that the transactions undertaken are in line with the customer's risk profile and business and, where necessary, examine the source of funds, to detect possible money laundering or terrorist financing. If appropriate, the risk rating of the customer should be raised or lowered. Where a customer was assessed as low risk during onboarding, but his actual activities involve a large number of wire transfers to unrelated parties in high-risk countries, this can be considered as not compatible with the customer's risk profile and the risk scoring of the specific customer may be raised to high-risk.

For example, a salaried person has frequent cash deposits into his or her bank account, in addition to the monthly salary, without an explanation in the client's file. In such a case, the bank should review the account for any suspicious outgoing transactions and request from the client to update his or her KYC documentation as something might have changed.

Another example would be of an investment holding company that normally makes few transactions over the year, and suddenly starts to make more frequent transactions that are instead trade related. Again, the Bank here should ask for an update of the client's KYC/CDD data. It is therefore important to keep client information up to date in a frequency that is appropriate to the AML risk of that particular client. Updating of client data should be supported by independent documentary evidence and not be deduced from transactions. In the example above, the obliged entity should not just deduce that the holding company has converted to a trading one but seek supporting evidence for this.

Firms should record and document their risk assessments of business relationships, as well as any changes made to risk assessments as part of their reviews and monitoring, to ensure that they can demonstrate to the competent authorities that their risk assessments and associated

risk management measures are adequate if requested. Obliged entities must also keep the documents, data or information they hold up to date, with a view to understand whether the risk associated with a business relationship has changed.

1.8 The risk-based approach in terrorist financing

Like in money laundering, when we apply the risk-based approach to terrorist financing, it requires identification and assessment of the terrorist financing risk. However, in terrorist financing, it is more difficult to do that because terrorist financing usually involves low value transactions and in many cases the funds come from legitimate sources, depending on the type of the terrorist organisation.

Traditional transaction monitoring mechanisms used for the identification of money laundering risks may be appropriate in cases where the financing of terrorism is derived from criminal activity. Where the funding of terrorism is from legitimate sources, it is more difficult to identify suspicious activity. For example, a terrorist may use funds to purchase some commonly used chemicals or a vehicle to conduct a terrorist attack.

Obliged entities are not required to identify the underlying criminal activity but must report possible suspicious activity. The FIU and law enforcement authorities will examine the report and they will decide whether a transaction is linked to terrorist financing or not.

2. Risk factors

When assessing and measure the level of risk of a business relationship with a client, a regulated firm need to take into consideration specific risk factor indicators:

- ✓ Customer risk factors
- ✓ Countries and geographical areas risk factors
- ✓ Product services and transaction risk factors
- ✓ Delivery Channels risk factors

Obliged entities should not only obtain information or documents for their KYC requirements, but they are required to understand these documents so as to obtain a holistic view of the risk associated with a business relationship or an occasional transaction.

Obliged entities should note that the following risk factors are not exhaustive, nor is there an expectation that firms will consider all risk factors in all cases. Firms should take a holistic view of the risk associated with the situation and note that the presence of isolated risk factors does not necessarily categorize a business relationship as high or low risk.

2.1 Risk-Based Approach risk factors

Customer risk factors

Customer risk factors are related to the types of customers whose characteristics might expose the business to lesser or greater degree of ML or TF risks. The key element in this case is to take appropriate measures to identify the customer and ensure to the extent possible that the customer is who he claims to be.

Obliged Entities are required to identify and assess the risk associated with their customers or the customer's beneficial owner. The beneficial owner is a person who ultimately owns or controls a legal entity or arrangement of 25% plus one share.

When assessing customer risk factors firms should consider:

- The customer's or the beneficial owner business or professional activity/ies
- The customer's or the beneficial owner's reputation
- The customer's or the beneficial owner's nature and behaviour

<u>The customer's or the beneficial owner business or professional activity/ies</u>

Obliged entities need to consider risk factors that may be relevant with regards to the business or professional activity of the customer, if the customer's or a customer's beneficial owner's business:

Factors related to the business or professional activity that increase risk are customers that:

- have links to sectors that are commonly associated with higher corruption risk, such as construction, pharmaceuticals and healthcare, the arms trade and defence, the extractive industries or public procurement.
- have links to sectors that are commonly associated with higher money laundering and terrorist financing risks such as casinos or dealers in precious metals.
- have links to sectors that involve significant amounts of cash.
- have links or connection with a Politically Exposed Person (PEP) or the beneficial owner is a PEP.

- have another prominent position or enjoys a high public profile that might enable him to abuse his position for private gain. Examples include public officials that are not PEPs but they have the ability to influence the awarding of public contracts, decision-making members or have the power to influence the government and other senior decision-makers.
- have been subject to supervisory sanctions or enforcement for failure to comply with AML/CFT obligations or wider conduct requirements in recent years

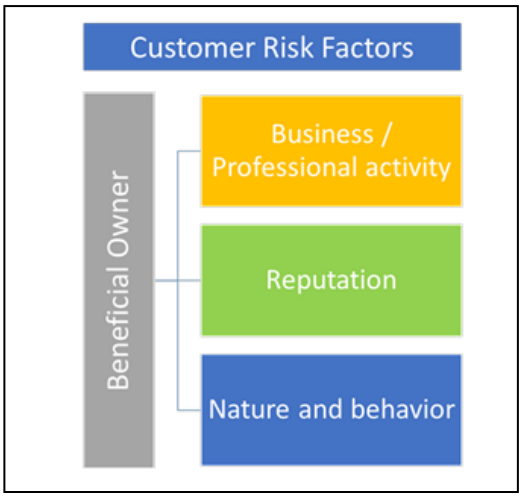
Special consideration is needed to identify whether the customer is a Politically Exposed Person (PEP). Additionally, obliged entities, as part of the risk-based approach need also to comply with the relevant sanctions law in their country to identify individuals, organisations or countries that are subject to sanctions.

Factors that decrease risk and may allow for specifically simplified due diligence measures include the following:

- The customer is a legal person subject to disclosure requirements and the information is publicly available. Examples include public companies listed on stock exchanges.
- The customer is a credit or financial institution acting on its own account which is effectively supervised.
- The customer is a public administration or enterprise from a jurisdiction with low levels of corruption.
- the customer's or the beneficial owner's background is consistent current with the customer's planned business activity, the source of funds and the customer's or beneficial owner's source of wealth.

<u>The customer's or the beneficial owner's reputation</u>

Examples of risk factors which may be relevant when considering the risk associated with a customer's or beneficial owners' reputation include:



- reliable and credible adverse media reports about the customer, any reliable and credible allegations of criminality or terrorism against the customer or the beneficial owner.
- if the customer or beneficial owner had his assets frozen due to administrative or criminal proceedings or allegations of terrorism or terrorist financing or was associated with an asset freeze.
- if the customer or the beneficial owner has been reported in the past for suspicious transactions.

The customer's or the beneficial owner's nature and behaviour

Risk factors that may be relevant when considering the risk associated with a customer's or beneficial owner's nature and behaviour include:

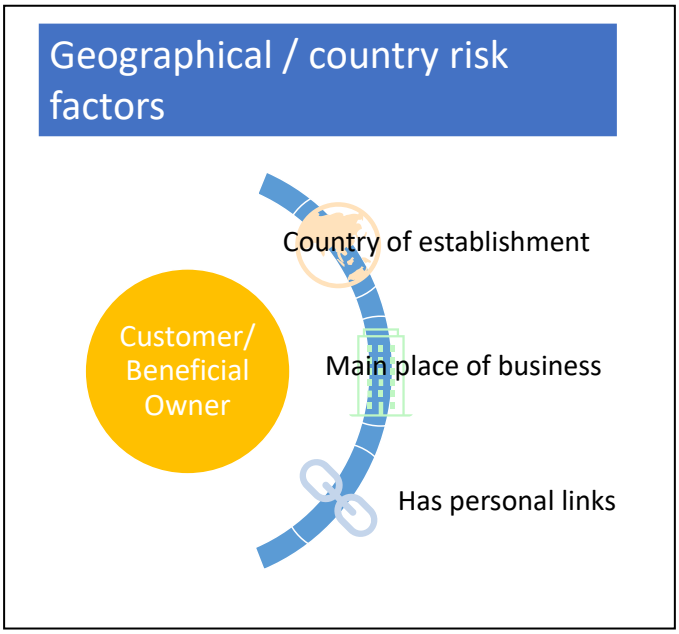
- The customer is unable to provide robust evidence of their identity. In some cases, there is legitimate reasons for that, for example asylum seekers.
- Whether there are doubts about the veracity or accuracy of the customer's identity.
- The customer avoids the establishment of a business relationship and is looking to carry out a one-off transaction while the establishment of a business relationship would make more economic sense.
- The customer's ownership and controls structure have to be transparent and make sense. If they are complex or opaque, is there an obvious commercial or lawful rationale?
- Customer that issue bearer shares or has nominee shareholders.
- The customer is an asset holding vehicle such as a private investment company.
- The customer request transactions that are complex, unusually, or unexpectedly large or have an unusual or unexpected pattern without an apparent economic or lawful purpose or a sound commercial rationale.
- The customer request unnecessary or unreasonable levels of secrecy or is trying to disguise the true nature of his business.
- The customer or the beneficiary's owner source of wealth or source of funds can be easily explained.
- The customer is a non-profit organisation that can be abused for terrorist financing purposes.

Geographical risk factors

When identifying the risk associated with countries and geographical areas, firms should consider the risk related to the jurisdictions in which the customer and the beneficial owner:

a. are based
b. have the main place of business
c. have relevant personal links.

Special consideration needs to be given to:



- countries identified by credible sources, such as mutual evaluations, detailed assessment reports or published follow-up reports, as not having effective AML/CFT systems
- countries identified by credible sources as having significant levels of corruption or other criminal activity
- countries subject to sanctions, embargos or similar measures issued by, for example, the Union or the United Nations
- countries providing funding or support for terrorist activities, or that have designated terrorist organisations operating within their country.

In the case where when a client is based or has links with a high-risk country according to the FATF or the European Commission, obliged entities should assign a high-risk classification to the client and enhanced due diligence measures.

Risk factors that need to be considered when identifying the effectiveness of a jurisdiction's AML/CFT regime include:

- whether the country has been identified as having strategic deficiencies in its AML/CFT regime and mutual evaluation reports by the Financial Action Task Force (FATF),
- whether the country complies with international tax transparency standards,
- whether the country where the funds used in the customer's account are generated, the extent predicate offences are prosecuted and the effectiveness of the legal system of the country to combat money laundering,
- whether in the country/ies where funds are received from or sent to, operate groups committing terrorist acts.
- Whether the country/ies is subject to sanctions or embargoes
- Whether it is a country having significant levels of corruption or other criminal activities such as narcotics, arm dealing, human trafficking, illicit diamond trading etc.

DID YOU KNOW?

Obliged entities are also allowed to perform their own individual risk assessments on countries and decide whether specific countries will be treated as high-risk or not.

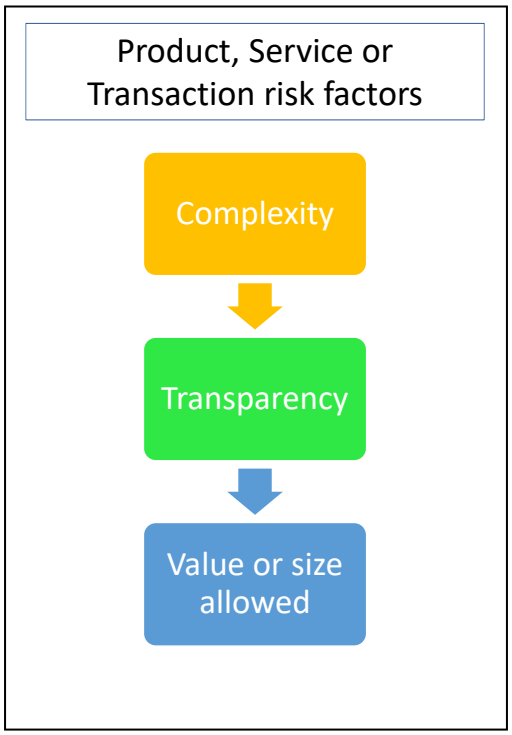
Obliged entities should note that the nature and purpose of the business relationship will often determine the relative importance of individual country and geographical risk factors. For example, where the funds used in a business relationship have been generated abroad, then the level of predicate offences to money laundering and the effectiveness of a country's legal system will be particularly relevant.

Obliged entities should note that, if a country is a member of the FATF or an FATF-Style Regional Body (FSRB) (e.g. MoneyVal) does not, of itself, mean that the jurisdiction's AML/CFT regime is adequate and effective.

Product, service or transaction risk factors

When identifying the risk associated with their products, services or transactions, firms should consider the risk related to:

a. the level of transparency, or opaqueness, the product, service or transaction affords,
b. the complexity of the product, service or transaction and
c. the value or size of the product, service or transaction.



According to FATF's recommendation 15, "a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies". This means that when an obliged entity enters new fields, such as new business products or services, it should evaluate these products or services' money laundering and sanctions vulnerabilities and implement appropriate controls before launching them into the market and take appropriate measures to mitigate the related risks.

Products or services that allow the customer or beneficial owner to remain anonymous or hide their identity are carrying a higher money laundering and terrorist financing risk. Examples include bearer shares, fiduciary deposits, offshore companies, trusts, foundations, shell companies or companies with nominee shareholders. Cryptocurrencies also provide anonymity and have been used in many cases by criminals to hide their illicitly gained proceeds of crime.

Complex transactions, transactions that involve multiple countries, multiple parties (financial intermediaries or brokers), product or services allowing payments from third parties, cash-intensive products or services or products or services encourage high-value transactions are also carrying a high money laundering and terrorist financing risk.

Products and services that indicate a potentially high money laundering and terrorist financing risks include:

- private banking,
- products or transactions that might favour anonymity,
- non-face-to-face business relationships or transactions, without certain safeguards (such as electronic signatures),
- payment received from unknown or unassociated third parties,
- new products and new business practices, including new delivery mechanism, and the use of new or developing technologies for both new and pre-existing products.

Products and services that indicate a potentially lower money laundering and terrorist financing risks include:

- life insurance policies for which the premium is low,
- insurance policies for pension schemes if there is no early surrender option and the policy cannot be used as collateral,
- a pension, superannuation or similar scheme that provides retirement benefits to employees, where contributions are made by way of deduction from wages, and the scheme rules do not permit the assignment of a member's interest under the scheme,
- financial products or services that provide appropriately defined and limited services to certain types of customers, so as to increase access for financial inclusion purposes,
- products where the risks of money laundering and terrorist financing are managed by other factors such as purse limits or transparency of ownership (i.e., certain types of electronic money).

These types of products and services, by their own nature, may carry less ML/TF risks than standard products and services, and make them eligible for exemptions from some AML/CFT controls or simplified due diligence measures depending on the extent of lower risks.

Delivery channel risk factors

This is the risk associated with the way the customer obtains the product or service. This includes the extent to which a business relationship is conducted:

- ✓ on a non-face-to-face basis or
- ✓ though introducers or intermediaries the entity might use.

When the customer is not physically present for identification purposes, there is a risk of identity fraud. For this purpose, the OE needs to ensure that is using a reliable form of non-face-to-face CDD that will allow the obliged entity to identify, verify and effectively monitor this type of clients and their beneficial owners.

Where the customer has been introduced from another part of the same group of the obliged entity, the obliged entity needs to ensure that the part of the group applies customer due

diligence, record-keeping requirements and the data protection polices of the group. It must also ensure that there is in place an AML/CFT program and is supervised at a group level.

An obliged entity is allowed rely upon a third party for KYC and CDD requirements. When the customer has been introduced by a third party, the obliged entity needs to be aware that the ultimate responsibility for effective customer due diligence application remains upon the obliged entity. It also needs to be satisfied that the third party is regulated, supervised, and has measures in place to comply with customer due diligence and record-keeping requirements. The obliged entity also needs ensure that copies of identification data and other relevant documentation relating to the CDD requirements will be made available by the third party to the obliged entity upon request and without delay.

Obliged entities, if allowed in the national regulations may rely on technological tools such as digital ID systems when applying their risk-based approach.

3. Risk Management

A simple definition of a risk is the potential of gaining or losing something of value. It is a broad definition, but it is appropriate in this case as the area of risk management is very subjective. Although a relatively simple concept, its application can be very challenging.

Risk management in the financial services sector is becoming of paramount importance in all areas and AML is not an exception. Identifying risks can be a very difficult task. Oftentimes entire scenarios may not be predicted by management. This makes organisations vulnerable in case these scenarios do materialize.

A regulated entity needs a risk management policy and procedures in place to address all the risks that would lead to compliance failure with its local regulatory framework concerning AML. Such compliance failure would impact the organisation negatively, financially through an administrative fine from the regulator, bad publicity in the press, losing the operating license or even imprisonment of executives or employees. AML risks are part of the Operational Risks for an organisation.

Some key AML risks for an organisation are: not having policies and procedures in compliance with local laws and regulations, failure to classify a client in the appropriate risk category, failure to report a suspicious transaction to the authorities or failure to freeze assets of a client on the sanctions lists.

Professional judgement must be exercised in determining the risks of an organisation. Risk determination must be led by the organisation's Compliance team. Input from the executives and other key staff members is required, in order to address as many risks as possible that could potentially cause damage to the organisation.

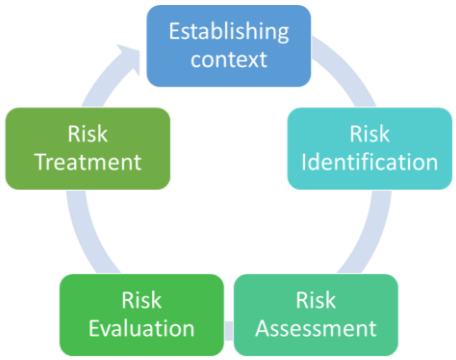
Risks should be identified and separately for each financial institution as part of an internal process, assessed based on impact and likelihood and evaluated against criteria set by top management, to create a risk management policy.

DID YOU KNOW?

A risk has two main elements, an impact, and a likelihood. Even in cases where the likelihood of the specific risk is small, but the impact will be large, action is required.

A foreign exchange trading company that is accepting many micro-investors, they start off with a small initial deposit. The likelihood of laundering money through such small amounts is very low but potentially the impact is large if such an event occurs. Action is required in this case to bring the risk to an acceptable level.

Risk management is an ongoing process consisting of five steps. Establishing the context, identifying the risk, assessing the risk, evaluating the risk, and treating it. A risk can either be avoided, prevented, reduced, shared, or simply accepted.



3.1 Risk management treatment

In order to perform a proper Risk Assessment for the organisation, there are two main areas to consider, namely the Inherent Risk and the Control Environment. These risks must be identified to have an effective risk management policy. The Inherent Risk is essentially the cost of doing business. For example, an insurance company is bound to have claims as it is the nature of its products and similarly a bank would have some loans that would default. Control Environment is the control structure of an organisation.

In the case of AML, the KYC procedures, screenings against the sanctions lists, staffing and training, governance, and oversight, are some of the key control elements in the organisation. Inherent Risks must be evaluated during the Risk Assessment stage. Since most financial institutions have more than one service line, then it would be appropriate to perform this internal exercise on a service-by-service basis or a business unit, as well as to the entire organisation at a top level.

There are several mitigation ways that can be used solely or in conjunction with one another, namely avoiding, preventing, reducing, sharing, or accepting a risk. There is no set list of risks, but these should be identified separately for each regulated entity as part of an internal process, assessed based on impact and likelihood, and evaluated against criteria set by top management.

4. Customer classification

Following its risk assessment, an obliged entity should categorize its business relationships and occasional transactions according to the perceived level of money laundering and terrorist financing risk. Firms should decide on the most appropriate way to categorize risk. This will depend on the nature and size of the firm's business and the types of money laundering and terrorist financing risk it is exposed to.

AML/CFT risk categories can be broken down into the following levels but other categorisations are possible:

- **High Risk** — The risks here are significant but are not necessarily prohibited. To mitigate the heightened risk presented, the financial institution should apply more stringent controls to reduce the ML/FT risk, such as conducting enhanced due diligence and more rigorous transaction monitoring. Countries that maintain a reputation for corruption or drug trafficking are generally considered high-risk. High-risk customers may include politically exposed persons (PEPs) or certain types of money services businesses or cash intensive businesses; high-risk products and services may include correspondent banking and private banking.
- **Medium Risk**—Medium risk represents the expected level of risk posed by a business relationship. This usually requires standard due diligence procedures.
- **Low Risk**—This represents the baseline risk of money laundering. Typically, low risk indicates normal, expected activity.

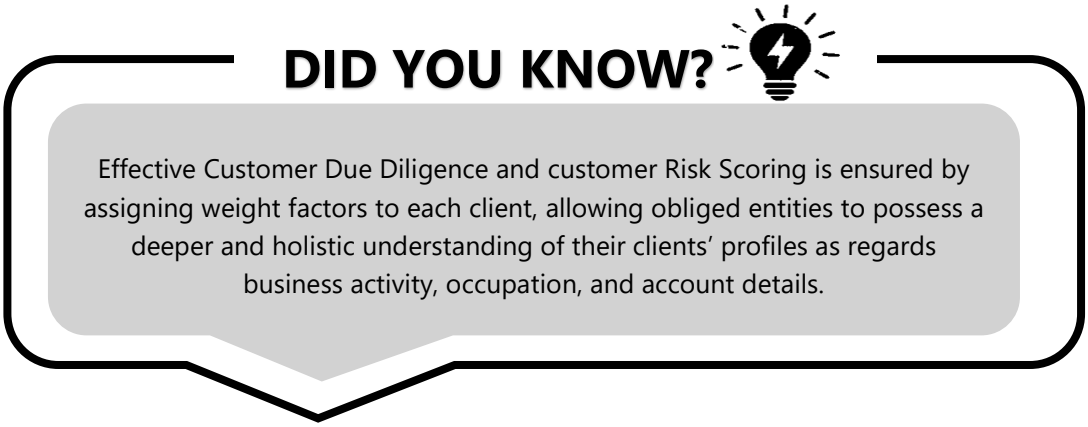
A money laundering or terrorist financing risk category can also be broken down to a "prohibited level". That means that the institution will not tolerate any dealings of any kind with the specific customer given the associated risk. This category could include transactions with countries subject to economic sanctions or designated as state sponsors of terrorism, such as those on the United Nations or Office of Foreign Assets Control lists.

4.1 AML/CFT Risk Scoring

A risk-based approach seeks to identify, manage, and analyse AML/CFT risk in order to design and effectively implement appropriate controls. As such, it is critical that risk ratings accurately reflect the present risks of an entity, provide meaningful assessments that lead to practical steps to mitigate the risks, and ensure that risk ratings are periodically reviewed and, when necessary, are updated.

A risk scoring model should be developed that will allow a regulated entity to apply appropriate weights to each risk factor, taking into consideration the money laundering risks

it faces. This model will allow a firm to allocate different 'scores' to different factors; for example, firms may decide that a customer's personal links to a jurisdiction associated with higher money laundering and terrorist financing risk is less relevant in light of the features of the product they seek.


DID YOU KNOW?
Effective Customer Due Diligence and customer Risk Scoring is ensured by assigning weight factors to each client, allowing obliged entities to possess a deeper and holistic understanding of their clients' profiles as regards business activity, occupation, and account details.

A risk-scoring model uses numeric values to determine the category of risk (geography, customer type and products and services), as well as the overall customer risk.

For example, each category could be given a score between 1 and 20, with 20 being the riskiest. The individual categories could be scored with 1-8 being normal risk, 9-16 being medium risk and 17-20 being high risk. Such a model is particularly helpful when looking at product risk, as it will help determine appropriate controls for the products. The three categories are then combined to give a composite score. A simple model would just add the totals from the categories, which would yield a score between 3 and 30. The model can be made more complex by weighting each of the factors differently, such as putting more emphasis on the type of customer, as opposed to the product or country. The model can be made even more sophisticated by, for instance, creating combinations of factors that will determine the overall rating. The degree of complexity is up to the institution; the more complex, the more likely the rating will reflect the customer's overall risk.

Example1: You have a small, foreign, private company that you do not have much information about, seeking to open a checking account with online wire transfer capabilities. That customer's ability to rapidly transfer funds raises its risk level. The customer may also have higher risk ratings for geography, customer type and products and services.

Example2: You have a publicly listed domestic company listed on a major stock market that wants to establish an employee retirement plan. Public companies are subject to disclosure requirements to be allowed to be listed on the major stock market, such as to provide adequate transparency of beneficial ownership. This type of customers has a lower money-laundering risk.

Example 3: Retirement plan accounts, such as pension schemes that have no early surrender option and cannot be used as collateral, are not very vulnerable to money laundering. As a

result, this customer and account will have a much lower risk that the above example of the foreign private company.

The next step is to determine what thresholds to establish for each risk category. The institution should be mindful that high-risk relationships should not represent a too large segment of the population; this is not to say the scores should be adapted to fit the customer portfolio, rather, because high-risk customers truly do need more attention. In addition, if the portfolio is overly weighted toward high-risk the overall risk level in the institution may be too great to support.

Assessing AML/CFT is an ongoing and evolving component of maintain a compliant AML/CFT program. Evaluating the risk scoring model and conducting the risk assessment itself may need to be performed annually, every eighteen to twenty-four months, before the launch of a new product, or when an acquisition of another financial institution occurs. Periodically reassessing risk-rating criteria will show if the customers that are scored as higher risk are actually more likely to engage in potentially suspicious activity.

The weight assigned to each risk factor to ascertain the overall total risk rating of each client is judgmental and based on the non-exhausting list of risk factors. The below table illustrates an example of a suggested applicable level of due diligence and monitoring of the business relationship:

Total Risk Scoring	**17-20**	**9-16**	**4-8**
Risk Level	High	Normal	Low
Due Diligence Level	EDD	CDD	CDD/SDD
Approval	BOD	MLCO	MLCO
CDD updates	Yearly, BOD approval for continuance of the relationship	Every 2 years	Every 3 years

Where a firm uses automated IT systems to allocate overall risk scores to categorize business relationships or occasional transactions and does not develop these in house but purchases them from an external provider, it should understand how the system works and how it combines risk factors to achieve an overall risk score.

A firm must always be able to satisfy itself that the scores allocated reflect the firm's understanding of money laundering and terrorist financing risk and it should be able to demonstrate this to the competent authority.

Risk is dynamic and needs to be continuously managed. It should also be noted that the environment in which each organisation operates is subject to continual change. Externally, the political changes of a jurisdiction i.e., when economic sanctions are imposed or removed may impact a country-risk rating. Internally, organisations respond to market and customer demands by introducing new products and services and implementing new delivery systems. The combination of these changes makes it critical that the money laundering and terrorist financing risk model is subject to regular review. In some countries, there is a legislative

obligation for such reviews to be undertaken on a regular basis — usually annually or when new products, delivery channels or customer types are introduced.

Another critical component of a risk assessment is having a process to re-evaluate risks and determine when the customer risk rating should be raised or lowered. Identifying the key factors that should trigger such a re-evaluation is essential to efficient allocation of limited resources. In addition to the initial assessment of the inherent risk of a customer, it is important to consider how a customer's relationship — and risk — with the institution changes over time. Perhaps the most important consideration driving a customer's risk rating is the actual activity that the customer conducts. For example: A student checking account may start out as low risk. But if records show that it is involved in a large number and volume of wires to higher risk jurisdictions, which indicates abnormal behaviour for this client type, the risk level for this account may need to be raised.

Similarly, a potentially higher risk customer such as a money transfer business (MTB), - otherwise known as money service businesses (MSB) – or a correspondent bank may be engaging in exactly the type of activity they indicate they will conduct. This customer may not be as risky as one might think based solely on the inherent risk. And so, the "low" or "standard" risk student customer based solely on inherent risk may actually present more risk to the institution than the MTB that presents a "high" inherent risk.

As every obliged entity develops transaction history with customers, it should consider modifying the risk rating of the customer, based on:

- Unusual activity, such as alerts, cases and suspicious transaction report (STR) filings.
- Receipt of law enforcement inquiries, such as subpoenas.
- Transactions that violate economic sanctions programs.
- Other considerations, such as significant volumes of activity where it would not be expected, such as a domestic charity engaging in large international transactions or businesses engaged in large volumes of cash where this would not normally be expected. The institution knowledge of the customer based on its activity will better determine the actual risk presented by a customer.

4.2 Weighting of risk factors

When weighting risk factors, firms should make an informed judgement about the relevance of different risk factors in the context of a business relationship or occasional transaction. This often results in firms allocating different "scores" to different factors. For example, firms may decide that a customer's personal links to a jurisdiction with higher money laundering and terrorist financing risk is less relevant in light of the features of the product the customer seeks.

When **weighting risk factors**, firms should ensure that:

- weighting is not unduly influenced by just one factor.
- economic or profit considerations do not influence the risk rating.

- weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk.
- they are able to over-ride any automatically generated risk scores where necessary. The rationale for the decision to over-ride such scores should be documented appropriately.

The weight given to each of these factors is likely to vary from product to product and customer to customer (or category of customer) and from one firm to another.

5. Learning summary

- The risk-based approach allows a firm to identify its risks and invest its resources in those areas that pose higher money laundering and terrorist financing risks.
- Countries are required to undertake risks assessments to identify money laundering and terrorist financing risks within their territories. These assessments will assist obliged entities to create their AML program.
- Firms' approach to assessing and managing the money laundering and terrorist financing risk associated with business relationships and occasional transactions should include business-wide risk assessments, CDD, obtain a holistic view of the business relationship and monitoring and review.
- Obliged entities need to assess each business relationship on a risk-based approach taking into consideration customer risk factors, geographical risk factors, product, service and transaction risk factors and delivery channel risk factors.
- A risk model should exist in every obliged entity that weights each factor appropriately and classify each business relationship according to its money laundering and terrorist financing risk.

6. End of Chapter Questions

Think of an answer for each question and refer to the chapter content for confirmation.

- ✓ What is the purpose of the risk-based approach?
- ✓ What is the Supranational risk assessment?
- ✓ What is the National risk assessment?
- ✓ What are the main risk factors to consider when assessing the money laundering and terrorist financing risk of a customer with regards to:
    - Customer risk
    - Geographical risk
    - Product, service, and transaction risk
    - Delivery channel risk

NOTES

Chapter 5

Customer Due Diligence (CDD)

Learning objectives

- Understand what Customer Due Diligence (CDD) is
- Learn the types of CDD and their application
- Learn about transaction monitoring and suspicious transaction reporting.

Introduction

Sound KYC procedures must be seen as a critical element in the effective management of financial risks. KYC safeguards go beyond simple account opening and record-keeping and require firms to have in place an acceptance policy and a solid identification and verification program that will enable firms to assess each potential customer at the time of the business relationship but also throughout the duration of the relationship.

Sound KYC standards are necessary to ensure market integrity and their necessity has been heightened by the direct and indirect losses incurred by firms, including major banks, due to their lack of diligence in applying appropriate procedures. These losses could probably have been avoided and damage to the firms' reputation would be significantly diminished if the firms had maintained effective KYC programmes.

The Basel Committee, FATF recommendations, and the European Supervisory Authorities (ESAs) have issued several guidance on the essential elements of KYC standards and their implementation. In a report[4] from the European Commission to the European Parliament and Council, the Commission reported that one of the challenges faced by the EU in tackling financial crime was firms' failure to perform adequate CDD on their customers. As a result, the reported noted some firms "...had insufficient understanding of their customers' actual operations and were ultimately unable to draw meaningful conclusions as to whether or not a customer's activity was suspicious".

The Basel's Committee paper provides guidance as to minimum standards for worldwide implementation for all banks. These standards may need to be supplemented and/or strengthened, by additional measures tailored to the risks of institutions and risks in the banking system of individual countries.

The need for rigorous customer due diligence standards is not restricted to banks. All non-bank financial institutions and professional intermediaries of financial services, such as lawyers

[4] European Commission, Brussels 24.07.2019 COM(2019) 373 Final, "Report from the Commission to the European Parliament and The Council on the assessment of recent alleged money laundering cases involving EU credit institutions"

and accountants, are exposed to money laundering and therefore need guidance to design their KYC program.

Sound KYC procedures have particular relevance to the safety and soundness of firms, in that:

- they help to protect firms' reputation and the integrity of the financial system by reducing the likelihood of firms becoming a vehicle for or a victim of financial crime and suffering consequential reputational damage;
- they constitute an essential part of sound risk management (e.g. by providing the basis for identifying, limiting and controlling risk exposures in assets and liabilities, including assets under management).

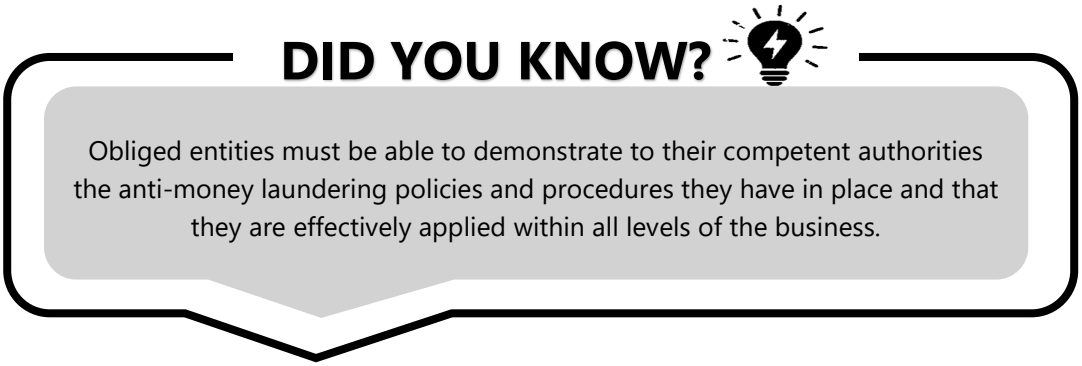
The inadequacy or absence of KYC standards can subject firms to serious customer and counterparty risks, especially reputational, operational, legal and concentration risks. It is worth noting that all these risks are interrelated. Even more, any one of them can result in significant financial cost to firms as well as the need to divert considerable management time and energy to resolving problems that arise.

In this Chapter, we will understand what the appropriate KYC and CDD procedures are and what they involve, not only for banks but for all entities that need to comply with anti-money laundering regulations. We will also examine when we obliged entities can apply simplified customer due diligence and in which cases should apply enhanced due diligence. We will also discuss about the application of KYC and CDD measures in cross-border activities.

1. Know Your Customer (KYC) and Customer Due Diligence (CDD)

It is important for obliged entities to have in place appropriate KYC and CDD procedures that will enable them to identify, verify the client, understand the nature and purpose of the business relationship, and effectively monitor customer accounts in order to identify possible suspicious transactions.

To perform a customer risk assessment, the firm must collect sufficient information with regards to the client to fully understand the potential money laundering and terrorist financing risks that may be linked with a customer. A key control to mitigate or reduce these risks is undertaking KYC on each individual customer, and in the case of legal entities or arrangements, such as companies or trusts, on the legal entity itself and its beneficial owners.


DID YOU KNOW?
Obliged entities must be able to demonstrate to their competent authorities the anti-money laundering policies and procedures they have in place and that they are effectively applied within all levels of the business.

According to FATF Recommendation 10, CDD measures must be applied when:

a. establishing business relations
b. carrying out occasional transactions above the applicable designated threshold (USD/EUR 15,000)
c. there is a suspicion of money laundering or terrorist financing
d. the financial institution has doubts about the veracity or adequacy of previously obtained customer identification data

Each country may determine how it imposes specific CDD obligations, either through law or enforceable means. Within EU and according to the 4th AML directive, CDD must be also conducted when in transfer of goods above €10,000 in cash and in gambling services transactions above €2,000.

When assessing the risk posed by the client and the type of CDD that will be applied to the customer, obliged entities should at least take into consideration,

- ✓ the purpose of the business relationship, the level of assets (amounts) deposited by the client
- ✓ the size of transactions undertaken,
- ✓ the regularity or duration of the business relationship.

1.1 When is KYC and CDD applied?

According to FATF Recommendation 10, firms "are required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. Countries may permit obliged entities to complete the verification as soon as reasonably practicable following the establishment of the relationship, where the money laundering and terrorist financing risks are effectively managed and where this is essential not to interrupt the normal conduct of business".

Following this recommendation, most AML/CFT regulations state that, save in the above exceptional circumstances, firms should not onboard or establish a business relationship with a new customer until the KYC and CDD on them can be undertaken. It is therefore important that firms carefully review local AML/CFT Regulations regarding these exceptions.

1.2 Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures

The purpose of CDD is to enable an obliged entity to have a complete picture of the client so as to identify irregular patterns in the customer activity that require scrutiny and might be subject to suspicious transaction reporting.

According to FATF recommendation 10, customer due diligence includes:

a. Identifying the customer and verifying that customer's identity using reliable, independent source documents, data, or information.
b. Identifying the beneficial owner and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is.
c. Understanding and, as appropriate, obtaining information on the purpose and intended nature of the business relationship.
d. Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the institution's knowledge of the customer, their business and risk profile, including, where necessary, the source of funds.

An appropriate CDD program is comprised of the following:

Customer Identification	Full identification and verification of the customer or the legal entity and its beneficial owners. This information must remain updated throughout the business relationship.
Economic profile	Identifying the customer's risk profile and expected account activity. This will enable the obliged entity to compare the expected movement of account with the actual.
Customer acceptance	Creation of the acceptance policy which includes the methodology of how to categorize customers with regards to the associated money laundering and terrorist financing risk. It also includes prohibited customers.
Risk classification	Taking into consideration the money laundering or terrorist financing risk on a risk-based approach, the customer is assigned with a risk scoring which must be regularly reviewed.
Monitoring	Monitoring of transactions according to the risk profile of the customer.
Suspicious Transaction Reporting	Identify unusual transactions or activities which are not consistent with the customer's profile and establishing procedures for reporting to the MLCO and the FIU

Firms must adjust the extent of initial CDD measures on a risk-sensitive basis. Where the risk associated with a business relationship is low, and to the extent permitted by national legislation, firms may be able to apply simplified customer due diligence measures (SDD). Where the risk associated with a business relationship is increased, firms must apply enhanced customer due diligence measures (EDD) and ongoing monitoring. The purpose of EDD is, for

clients who have a high money laundering risk, the obliged entity to be able to bring the risk to an acceptable level.

Firms should gather sufficient information to be satisfied that they have identified all relevant risk factors, deriving from a specific relationship to decide the level of CDD measures to be applied to the specific customer. The purpose is to obtain a holistic view of the risk associated with a business relationship before they decide on the extent and level off CDD measures to be applied.

Firms are required to adopt a risk-based approach and ensure that an appropriate level of CDD is applied to all customers, new and existing, on an ongoing basis. Where an obliged entity is unable to comply with the above requirements on a risk-based approach, for example, is unable to identify a new client satisfactorily, it must not open an account or commence a business relationship or transaction. It must terminate the business relationship and consider making a suspicious transaction report in relation to the customer.

1.3 Customer Onboarding and Know Your Customer (KYC)

Having appropriate KYC procedures is a regulatory obligation of financial and non-financial organisations. Obliged entities need to develop customer identification and verification processes of their customers on a regular basis. KYC compliance prevent businesses from reputational damage, penalties, help the business to fight fraud, and mitigate financial crimes such as money laundering, terrorist financing.

Firms, need to take appropriate KYC measures when establishing business relationships with:

- Corporate vehicles
- Trust, nominee, and fiduciary accounts
- Introduced business
- Client accounts opened by professional intermediaries (for banks)
- Politically Exposed Persons (PEPs)
- Non-face-to-face clients
- Correspondent banking

The first step of CDD when establishing a business relationship with a client to take appropriate KYC measures to ensure that the customer is who he claims to be. This includes:

- obtaining information about the identity of customer (and its owners where it is not an individual) and
- verifying the accuracy of that information.

For individuals, the identification process is when the customer provides information on onboarding, when the customer requires the opening of an account. The verification process involves obtaining a document from an “independent and reliable source”. This includes a proof of identity such as a passport, identity card or photo-driving license (depending on the national law of each country) to verify the client's name, date of birth and nationality, and a proof of address, such as a recent utility bill to confirm address. On onboarding, additional CDD information are required to establish the nature and the purpose of the business

relationship. This includes the occupation and how they plan to use the products and services offered by the firm to name a few. The level of CDD undertaken on a customer will vary, both on AML regulatory requirements and the level of possible money laundering risk that might be associated with the customer.

For legal persons, the standard information required on onboarding are:

Information for Identification	**Verification documents**
Name	Certificate of incorporation
Legal form and proof of existence	Certificate of good standing / partnership agreement / trust deed
Powers that regulate and bind the legal person	Memorandum and Articles of Association
Names of senior managers (or shareholders)	Certificate of shareholders (if any)
Address of the registered Office	Certificate of registered address

For legal persons, an obliged entity should also receive a resolution for account opening and operation and perform KYC on the persons authorised to operate the account, registered shareholders, and beneficial owners. When beneficial owners cannot be identified and verified, the firm can identify and verify the senior managers.

Obliged entities require that firms should also undertake KYC and CDD on the following:

- the person or entity that maintains an account with the firm or those on whose behalf an account is maintained (i.e., the beneficial owners) or the persons who will be accessing the products and services offered by the firm.
- The beneficiaries of transactions conducted by professional intermediaries and
- Any person or entity connected with a financial transaction who can pose a significant reputational or other risk to the firm.

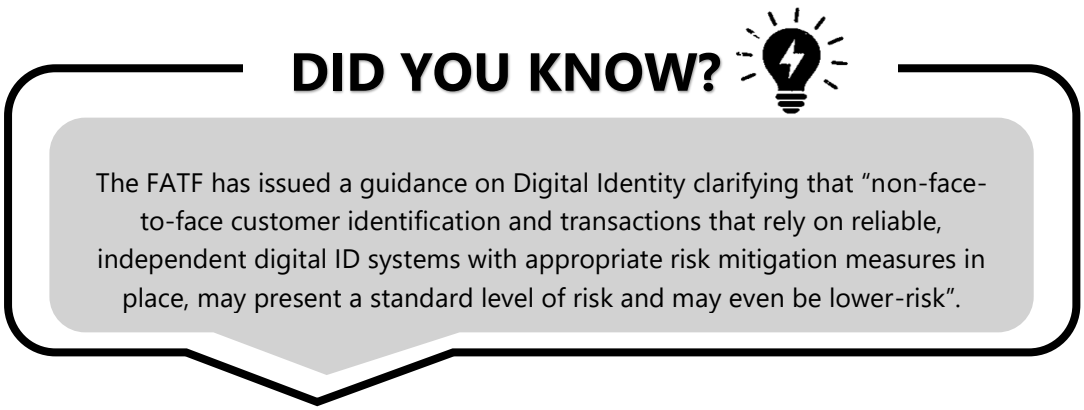
In the case of trusts, obliged entities need to identify and verify:

- the settlor (also known as trustor)
- the trustee(s)
- the protector (if any)
- the beneficiaries or class of beneficiaries
- any other natural person that exercises effective control over the trust.

For other types of legal arrangements, the obliged entity must identify and verify the identity of persons in equivalent positions.

The FATF recommendation 10 requires obliged entities to verify their customers' identities using "reliable and independent source". For this purpose, many obliged entities are equipped with technological tools proportionate to their size and complexity of their business to automate the identification and verification of the customers and other customer due

diligence obligations. If an obliged entity relies on technology for these tasks, the digital ID system used should employ adequate governance, processes and procedures that provide appropriate levels of confidence that the system produces accurate results.


DID YOU KNOW?
The FATF has issued a guidance on Digital Identity clarifying that "non-face-to-face customer identification and transactions that rely on reliable, independent digital ID systems with appropriate risk mitigation measures in place, may present a standard level of risk and may even be lower-risk".

Firms should never agree to open an account or conduct ongoing business with a customer who insists on anonymity or who gives a fictitious name. Nor should confidential numbered accounts function as anonymous accounts, but they should be subject to exactly the same KYC procedures as all other customer accounts, even if the test is carried out by selected staff. Whereas a numbered account can offer additional protection for the identity of the accountholder, the identity must be known to a sufficient number of staff to operate proper due diligence. Such accounts should in no circumstances be used to hide the customer identity from a firm's compliance function or from the supervisors.

There are cases where a customer requests the transfer of a balance from an account in the customer's name in another firm. The fact that the other firm is subject to the same KYC standards may provide some comfort, firms should nevertheless consider the possibility that the previous account manager may have asked for the account to be removed because of a concern about dubious activities. Naturally, customers have the right to move their business from one firm to another. However, if a firm has any reason to believe that an applicant is being refused financial services by another firm, it should apply enhanced diligence procedures to the customer.

Case Study

At High Hopes Capital LLP, a small investment management firm recently authorized by the FCA, David Little has been designated with the job of investor relations. The firm operates and manages one hedge fund and has raised £35m to date.

The fund remains open to new investment and one morning David is approached by Hedge Network Partners (HNP), an unregulated marketing consultant offering to act as an agent and market the fund to his hedge fund eligible client base for a reasonable success fee.

The arrangement sounds attractive to both parties and six weeks later, the investment consultant comes back to David with a definite interest from his clients.

The total of each individual investment is likely to exceed £60m. Each investment is in the client's name and therefore HNP is eligible to receive a sizeable commission.

Whilst the prospect of such a large capital injection is very exciting, David is mindful of the anti-money laundering issues and approaches HNP regarding the issue.

The directors of HNP are very understanding and within a few days a large parcel arrives, containing copies of HNP's certificate of incorporation, a recently audited report & accounts, personal identification papers (copy of passports, driving licenses etc.,) for each director.

There are also details of other city relationships, where reference can be sought.

David, deciding extra vigilance may be appropriate given the size of the investment, requests additional personal identification on HNP's directors and takes up two of the references.

HNP appears to be totally legitimate and David arranges with the fund administrator to start receiving the cheques from HNP's clients. These are then banked and invested into the hedge fund. In this situation, David appears to have been particularly vigilant in checking Hedge Network Partners' credentials.

Has David followed the correct due diligence procedures?

David has followed the right procedures in correctly identifying the agent, Hedge Network Partners and its' directors. It is clear, however, that HNP is unregulated and is acting as an agent for a number of underlying clients. The FCA would have expected High Hopes Capital LLP to have undertaken KYC checks and sought sufficient evidence of identity against each individual investor.

The fund administrator may act as a further 'checkpoint' before the cheques are cashed and the subsequent investments made.

2. Simplified and Enhanced Due Diligence measures

2.1 Simplified due diligence (SDD)

Countries may decide to apply simplified due diligence measures where:

- ✓ There is a proven low risk of money laundering or terrorist financing
- ✓ A financial activity other than the transferring of money or value, is carried out by a natural person on an occasional or very limited basis that there is low money laundering and terrorist financing risk.

This means that, where a customer relationship or occasional transaction appears to present a lower risk of financial crime, firms may be able to undertake CDD that is less extensive as would be the case for customers where elevated financial crime risks may be present.

Recommendation 10 of the FATF and national AML/CFT regulations specify the circumstances under which SDD may be undertaken. This means that the use of SDD is much more restricted. Some examples of business relationships that may be eligible to SDD measures include:

- public companies listed in a stock exchange and subject to disclosure requirements (either by stock exchange rules or through law or enforceable means), which impose requirements to ensure adequate transparency of beneficial ownership,
- public administrations or enterprises,
- customers that are resident in geographical areas of lower risk,
- other low-risk situations.

SDD is not an exemption from any of the CDD measures**.** When applying SDD, firms may:

a) **adjust the timing of CDD**, for example verifying the customer's identity during the establishment of the business relationship or verifying the customer's identity once transactions exceed a defined threshold or once a reasonable time limit has lapsed.

b) adjust the quantity of information obtained for identification, verification or monitoring purposes, for example by verifying the identity of the client on the basis of information obtained from one reliable, credible and independent document or data source only.

c) adjust the quality or source of information obtained for identification, verification or monitoring purposes, for example by accepting information obtained from the customer rather than an independent source when verifying the beneficial owner's identity; or where the risk associated with all aspects of the relationship is very low, relying on the source of funds to meet some of the CDD requirements, for example where the funds are state benefit payments.

d) adjust the frequency of CDD updates and reviews of the business relationship, for example carrying these out only when trigger events occur such as the customer looking to take out a new product or service or when a certain transaction threshold is reached.

e) adjust the frequency and intensity of transaction monitoring, for example by monitoring transactions above a certain threshold only. Where firms choose to do this, they must ensure that the threshold is set at a reasonable level and that they have systems in place to identify linked transactions that, together, would exceed that threshold.

It is important to remember that national AML/CFT regulations may include additional restrictions or requirements that must be met before a firm can perform SDD on a customer.

The information a firm obtains when applying SDD measures must enable the firm to be reasonable satisfied during assessment that the risk associated with the relationship is low and this can be justified. The information must also be enough to give the firm enough information about the nature of the business relationship to identify any unusual or suspicious transactions. SDD does not exempt an institution from reporting suspicious transactions to the FIU.

Where there are indications that the risk may not be low, for example where there are grounds to suspect that money laundering and terrorist financing is being attempted or where the firm has doubts about the veracity of the information obtained, SDD must not be applied. Equally, where specific high-risk scenarios apply and there is an obligation to conduct EDD, SDD must not be applied.

2.2 Enhanced Due Diligence (EDD)

Where the money laundering and terrorist financing risk associated with a business relationship is higher than in normal circumstances, the obliged entity needs to apply stringent measures to reduce the money laundering and terrorist financing risk or the business relationship with the client to an acceptable level. EDD measures cannot be substituted for regular CDD measures but must be applied in addition to regular those CDD measures.

Based on the FATF Recommendations, most national AML/CFT regulations prescribe or require that certain types of relationships automatically be treated as high risk. These include:

- Customers and/or the owners, close associate or family members are identified as a high-risk politically exposed person (PEP)
- Customers resident in, operating in or with a close connection to a jurisdiction identified by either the FATF or other national AML/CFT supervisors as being high risk (i.e., EU List of High Risk Third Countries)
- Cross-border correspondent relationships with a respondent institution based in a high-risk country

Obliged entities must also conduct EDD when dealing with:

- complex and unusually large transactions, or unusual patterns of transactions, that have no obvious economic or lawful purpose.
- Other cases established by national legislation.

Politically Exposed Persons (PEPs)

A PEP are high-profiled individuals who hold a public prominent function. These persons have power and have higher chances of abusing their position. They can also use their influence for personal gain instead for the benefit of the public. Also, they are vulnerable to bribes and may embezzle funds for public work projects. Obliged entities need to treat as PEPs family members and close associates of PEPs. It is extremely important for obliged entities to identify these individuals and manage the risks related to this type of business relationships.

However, not all PEPs are equal. Some PEPs are considered to have a higher risk than others and require additional scrutiny. According to the FATF guidance, on PEPs there are five types of PEPs:

- **Foreign PEPs**: individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior

politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.

- **Domestic PEPs**: individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations, important political party officials.
- **International organisation PEPs**: persons who are or have been entrusted with a prominent function by an international organisation (i.e., FIFA, UEFA etc.), refers to members of senior management or individuals who have been entrusted with equivalent functions, i.e., directors, deputy directors and members of the board or equivalent functions.
- **Family members** are individuals who are related to a PEP either directly (consanguinity) or through marriage or similar (civil) forms of partnership. Countries need to include in their national legislation which family members of a PEP constitute a PEP.
- **Close associates** are individuals who are closely connected to a PEP, either socially or professionally.

The EU 4th AML Directive does not differentiate between foreign and domestic PEPs. However, following the FATFs guidance, the 5th AML directive requires EU Member States to issue a list of specific functions which qualify as prominent public functions (public functions that are considered politically exposed). The same will happen in an EU level. These lists will be publicly available.

Obliged entities that have identified that a customer or beneficial owner is a **PEP** must always:

- ✓ Take adequate measures to establish the source of wealth and the source of funds to be used in the business relationship in order to allow the firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity.
- ✓ Obtain senior management approval for entering into, or continuing, a business relationship with a PEP.
- ✓ When considering whether to approve a PEP relationship, senior management should base their decision on the level of money laundering and terrorist financing risk the firm would be exposed to if it entered into that business relationship and how well equipped the firm is to manage that risk effectively.
- ✓ Apply enhanced ongoing monitoring of both transactions and the risk associated with the business relationship. Firms should identify unusual transactions and regularly review the information they hold to ensure that any new or emerging information that could affect the risk assessment is identified in a timely fashion. The frequency of ongoing monitoring should be determined by the level of high risk associated with the relationship.

When dealing with PEPs (or their family members or close associates), obliged entities must have procedures in place to identify these people and take appropriate measures to mitigate the risk associated with this specific type of business relationship.

These measures should apply for the subsequent 12 months from the moment a person will no longer be a PEP. However, after the end of 12 months, the obliged entity needs to perform again a risk assessment to decide whether the specific individual should continue to be treated as a PEP.

High-risk third countries

Obliged entities are required to apply EDD when dealing with customers that are natural or legal persons having links with countries identified as having strategic deficiencies in their money laundering and terrorist financing regime. The FATF has issued a list of countries subject to a call of action and jurisdictions under increased monitoring. The list includes countries under increased monitoring by FATF that are expected to resolve their strategic deficiencies within agreed timeframes.

The European Commission has also issued a high-risk third country list which considers the work of the FATF. Obliged entities within the EU jurisdiction, when dealing with natural persons or legal entities from high-risk third countries, need to apply enhanced due diligence measures. However, the specific measures are at the discretion of each Member State to decide. This fact creates certain problems and could also lead to a regulatory arbitrage. Therefore, it is essential to follow a harmonized approach, for example, with a look to the measures proposed by FATF.

Correspondent relationships

Correspondent banking is the provision of banking services by one bank (the "correspondent bank") to another bank (the "respondent bank"). Usually, large, international banks act as correspondents for thousands of other banks around the world, providing a wide range of services, international wire transfers, cheque clearing, payable-through accounts, and foreign exchange services.

Correspondent banks must take specific EDD measures where they have a cross-border correspondent relationship with a respondent institution that is based in a third country. The extent of these measures should also be adjusted on a risk-sensitive basis. We will examine further details with regards to correspondent banking in Chapter 7.

Unusual transactions

Obliged entities should have in place adequate policies and procedures to detect unusual transactions or patterns of transactions. They should be able to examine as far as reasonably possible the background and purpose of all complex, unusual large transactions and all unusual patterns of transactions that have no apparent economic or lawful purpose. Where the money laundering and terrorist financing risk is higher, EDD must be applied. They should also increase the degree and nature of monitoring of such a business relationship to determine whether the activities are usual or suspicious.

EDD measures must be applied where a firm detects transactions that are unusual because:

- they are larger than what the firm would normally expect based on its knowledge of the customer, the business relationship, or the category to which the customer belongs
- they have an unusual or unexpected pattern compared with the customer's normal activity or the pattern of transactions associated with similar customers, products or services; or
- they are very complex compared with other, similar, transactions associated with similar customer types, products, or services,
- the firm is not aware of an economic rationale or lawful purpose or doubts the veracity of the information it has been given.

These **EDD** measures should be sufficient to help the firm determine whether these transactions give rise to suspicion and must at least include:

- ✓ taking reasonable and adequate measures to understand the background and purpose of these transactions, for example by establishing the source and destination of the funds or finding out more about the customer's business to ascertain the likelihood of the customer making such transactions; and
- ✓ monitoring the business relationship and subsequent transactions more frequently and with greater attention to detail.

2.3 Application of EDD measures

When dealing with high-risk situations, firms should take an informed decision about which EDD measures are appropriate for each high-risk situation. The appropriate type of EDD, including the extent of the additional information sought, and of the increased monitoring carried out, will depend on the reason why an occasional transaction or a business relationship was classified as high risk.

EDD measures firms should apply may include:

- Increasing the quantity of information obtained for CDD purposes
- Increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity
- Increasing the frequency of reviews to be satisfied that the firm continues to be able to manage the risk associated with the individual business relationship

Examples include:

- Obtaining additional information on the customer (e.g., occupation, volume of assets, information available through public databases, internet, etc.), and updating more regularly the identification data of customer and beneficial owner.
- Obtaining additional information on the intended nature of the business relationship.
- Obtaining information on the source of funds or source of wealth of the customer.
- Obtaining information on the reasons for intended or performed transactions.
- Obtaining the approval of senior management to commence or continue the business relationship.
- Conducting enhanced monitoring of the business relationship, by increasing the number and timing of controls applied, and selecting patterns of transactions that need further examination.
- Requiring the first payment to be carried out through an account in the customer's name with a bank subject to similar CDD standards.

3. Other CDD Obligations

3.1 Record keeping requirements and data retention

Following FATF's guidance, countries should require obliged entities within their territories to take steps to maintain and retain specific records for a period of 5 years after the end of the business relationship.

Obliged entities should also keep and retain customers' assessments as well as the underlying factors under review to ensure these assessment remains up to date and relevant as part of their ongoing monitoring.

Records should also be kept for each individual transaction carried out during the business relationship of each client or for occasional transactions. These must be retained for five years from the date on which all activities on that transaction were completed.
All Internal suspicious reports made by staff and external reports to FIUs must also be retained and made available for inspection if required by the relevant competent authority.

Record-keeping procedures must be in please with measures to ensure that an obliged entity will be able to fully investigate possible suspicious activity that may arise several years after a business relationship with a customer has commenced. It will also ensure that the obliged entity will be able to comply with requests for information about customers from either the AML regulator or the local FIU. More recently, data retention has also proven valuable for firms to undertake data analytics of customer activity, use of products and services and adjust the controls used in their AML compliance programs to address emerging risk areas.

After the lapse of the five years, all records must be deleted, and hard copies must be destroyed. In case of a pending AML investigation, the firm is obligated to keep customer's data for another five years.

Banks, according to Basel Committee's Guidance, should develop "*clear standards on what records must be kept on customer identification and individual transactions and their retention period*". Such a practice is essential to permit a bank but also other obliged entities to monitor their relationship with the customer, to understand the customer's on-going business and, if necessary, to provide evidence in the event of disputes, legal action, or a financial investigation that could lead to criminal prosecution.

3.2 Monitoring of transactions

The Wolfsburg Group identifies monitoring as the automated or manual process of monitoring transactions after their execution in order to identify unusual transactions, including monitoring single transactions as well as transaction flows, for subsequent review and, where appropriate, reporting to the authorities. However, without appropriate KYC and CDD data, transaction monitoring becomes ineffective.

When onboarding a client, the obliged entity collects information and then verifies this information. The data obtained from the KYC and CDD procedures of the financial institution is of great importance for account monitoring purposes over the duration of the client relation.

Obliged entities are required to identify suspicious activities that may be related to money laundering, bribery and corruption, terrorist financing, or another form of financial crime. KYC and CDD information is used to create an economic profile for each customer with the purpose to establish what is the normal and reasonable activity of its customer and the expected turnover of the account. Any significant deviation from this economic profile and if there is suspicion, the employees should report their suspicion to the MLCO. The MLCO must investigate further and, where appropriate, consider making a Suspicious Transaction Reporting to the FIU.

Monitoring of customers transactions must be made on a daily basis and in real-time. The Wolfsburg Group notes that real-time payment screening is the process of screening or filtering relevant payment instructions prior to execution. Screening is a critical step in ensuring that an individual or a corporation does not facilitate criminal activity. Screening needs to take place at on-boarding but also during the business relationship with a customer. It is necessary to identify payments to or from persons or entities that may be related to sanctions or embargoes. A real-time payment screening is a preventive system of filtering payment instructions before their execution, against blacklists as aforementioned. On the other hand, a dedicated automated transaction system can compare account transaction activity during one period, against a previous period, and to issue alerts if there is an unusual activity. The check is done after the transaction is executed. These alerts are manually monitored by the operational staff to either suppress the alert or escalate the case further. Regardless of the action taken, there should be an audit trail in the system to log all actions and comments by the staff.

Monitoring and screening allow a firm to identify money laundering risks before they become threats. Continuous monitoring is required to enable the firm to identify any customers that require a modification in their risk scoring and now need to be treated as high risk, but also detect unusual or suspicious transactions that may occur during the business relationship with a client.

No two obliged entities are identical and the same is true for their internal control systems. The most common difference between internal controls systems is their size. For example, a small investment firm with five staff members and not more than a hundred managed client accounts cannot justify the cost of an automated-transaction-monitoring system as the case would be for a large international investment bank.

The Compliance Department and the MLCO should oversee the transaction monitoring process and perform reviews. Certain sophisticated systems can also allow a custom risk scoring system by the organisation to be applied against the transactions. If a manual system is going to be used, due to low volume, the staff essentially does the screening and monitoring at the same time but prior to execution. Part of the monitoring system of the financial institution is to provide exceptions that seek further investigation and if appropriate, to report suspicious transactions by filing an STR.

An obliged entity must also refrain from carrying out transactions which are known or suspected to be related to money laundering or terrorist financing unless instructed by the FIU. However, if this is impossible or likely to frustrate the beneficiaries by not carrying out the transaction, then the FIU must be informed immediately after execution. If a suspicion is made as part of an audit well after the execution, then it must still be reported. Furthermore, disclosure to the FIU of client information does not constitute a breach of any restriction on disclosure of information.

Monitoring wire transfers

Transferring money between jurisdictions is very common and is in most of the cases this method is used for legitimate purposes. However, it is a common practice during the layering stage of money laundering. For example, a person may place large sums of cash in a country with laxer money laundering regulations and then transfer the funds to any other country in the world. Obliged entities should therefore ensure that they require accurate originator information and beneficiary information on wire transfers and other related messages. It is important for such information to remain with the wire transfer or related message throughout the payment chain, as supporting evidence, and provide a clearer picture to the financial institution and the regulator as part of a possible audit or investigation.

Wire transfers also play an important role in the application of international or local sanctions or other freezing orders issued by local government and courts for both, incoming and outgoing transfers of funds. With the modern automation of wire transfers, it is therefore very important for a financial institution to have in place automated filtering systems for the transactions and prompt updating of blacklists whenever there is a data update. The aforementioned requirement for information for the originator and beneficiary is also crucial in order to cross check this information against these lists. A financial institution should have

in place a monitoring system that is appropriate to its nature of operations and size, considering relevant risks.

An independent internal audit is appropriate to test, not only the firm's internal policies and procedures but also the internal transaction monitoring system and perform appropriate testing. The ultimate responsibility for having an effective internal control system to handle AML issues lies with the Board of Directors.

3.3 Suspicious Transaction/Activity Reporting (STR/SAR)

Suspicious transaction or activity reporting is a requirement found in all AML regulations and is an important control in a firm's AML compliance program. It describes the process that must be followed when a member of the staff of an obliged entity has a suspicion that a transaction or an account activity may be related to a financial crime. They allow a firm to assess and report possible criminal activity to local authorities such as the FIU, who in turn, can take steps to investigate and intervene in criminal activity underway.

There should be in place a procedure that requires its staff to report any "suspicious activity", internally to the MLCO, when they know or suspect, or have reasonable grounds for knowing or suspecting, that another person is engaged in money laundering or the financing of terrorism or any other financial crime. When reporting a suspicious transaction to the MLCO, the staff member must properly document his or her rationale for suspicion. The reporting is filed directly and confidentially along with supporting documentation.

There are unlimited types of suspicious transactions. However, there are a number of "red flags" that might be an indication of suspicion for money laundering and terrorist financing. This includes transactions that are inconsistent with the customer's economic profile or activity. Staff members of the obliged entity must be vigilant on any suspicious transactions by clients. Recognizing a suspicious transaction is extremely important, both for the member of staff and the financial institution. Staff must receive training that will enable them to identify the signs or "red flags" related to a customer's behaviour or transactions, that could give rise to a suspicion.

With an ever-increasing frequency of financial transactions, the use of sophisticated automated systems for detection of suspicious transactions has become the norm. In these cases, the system raises red flags for certain transactions which must be reviewed by both operational and AML staff. Any suspicious transactions that cannot be explained by the operational staff as normal client business must be escalated to the MLCO.

Employees need to report to the MLCO without delay anything that comes to their attention in relation to transactions or activities for which there is a slight suspicion of money laundering or terrorist financing through STRs / SARs to the MLCO. They also need to understand that they can be personally liable for failure to report such suspicion. Failure to make a report "as soon as practicable" could well be a criminal offence.

A financial institution should have a process whereby any member of staff can raise a suspicion for a transaction and such a report should be filed directly and confidentially to the designated

MLCO along with supporting documentation. The MLCO is then responsible for investigating the suspicion and must clarify the situation with the reporting employee. The MLCO then has the final responsibility to send the report to the FIU directly and coordinate with them on any issues that might arise.

Although the financial institution may have certain monetary thresholds in an automated system, if a suspicion is raised for a transaction that is below these thresholds, then regardless of an amount, a report to the FIU must still be made.

Communication between the financial institution and the Financial Intelligence Unit (FIU) is key in apprehending persons who are laundering money through the financial system or using funds for terrorist activities. The communication channel is reporting from the financial institution's MLCO to the FIU through a Suspicious Transaction Report (STR).

All suspicious transactions, including attempted transactions, shall be reported by the financial institution as an STR to the FIU. In addition, the financial institution must also promptly respond to any requests by the FIU for additional information whether it relates to a case raised by the financial institution itself, or as part of another investigation conducted by the FIU.

DID YOU KNOW?
When an employee has reported a suspicious transaction internally to the MLCO the employee has fulfilled his/her legal obligation with regards to reporting suspicious transactions or activities.

Obliged Entities and their directors and employees must not notify the customer concerned or other third persons the fact that information regarding suspicious transactions is being, will be or has been transmitted to The Unit, concerning money laundering and terrorist financing. This is considered as "tipping-off" and is a criminal offence. Further, it is not allowed for any person to make any disclosure which may cause obstruction or negatively interfere with interrogations and investigations carried out while it knows or suspects that such interrogations and investigations are under way. Staff need to be provided with specific guidance on how to respond to client queries with regards to transactions under investigation

Firms must establish arrangements for training all employees as to their reporting obligations. This will usually be accompanied by a clear indication of disciplinary action against anyone who fails, without reasonable cause, to report suspicious transaction. Lack of adequate training can provide a defence for an employee who is charged with the offence of "failure to report" suspicious activity. However, if an individual relies on this defence, the firm may potentially face action for breaching the legal obligation to train all relevant employees.

No financial institution can reasonably be expected to detect all wrongdoing by customers, including money laundering. But if a financial institution develops systems and procedures to detect, monitor and report the riskier customers and transactions, it will increase its chances of staying out of harm's way from criminals and from government sanctions and penalties.

All records of Internal Suspicious Transaction / Activity Reports made by staff, and all MLCO external reports to FIU and/or law enforcement agencies, must be retained. This means that even if an internal suspicious report was not disclosed to the FIU, the original record must be maintained and made available for inspection if required by the AML regulator or FIU at a future date.

The reporting obligations are not limited to staff who are employed on a full-time basis. Consultants, contractors, and agents of the firm must also submit an Internal Suspicious Transaction, when required. This means that firms must ensure that all parties who work for or on behalf of the obliged entity understand this reporting obligation. Everyone needs to be aware who the MLCO is (to whom the reports must be submitted). This reporting obligation extends to the activities of any person, where such knowledge/suspicion comes or should come in the course of the business activities.

However, notaries and legal professionals, when they are assessing the position of their clients and when they are defending or representing them, are not obliged to perform suspicious transaction reporting.

FATF Recommendation 21 obliges countries that their financial institutions, their directors, officers and employees should be 'protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the Financial Intelligence Unit (FIU), even if they did not know precisely what the underlying criminal activity was, and regardless of whether illegal activity actually occurred'

This means that, when someone is making an internal suspicious report or disclosing to the FIU details of a suspicious transaction it is not considered to breach any confidentiality obligation with his or her client. Disclosure of information in good faith, even if an illegal activity has not actually occurred, does not constitute a breach of any restriction of disclosure of information imposed by other regulations.

3.4 Reporting of suspicious transactions in EU and the US

In the US, each member state has its own FIU. For example, in the UK it is the National Crime Agency or NCA. In the US the general requirements for reporting are not that different from the EU. After all, they both follow FATF's recommendations. However, there are some variations.

One additional requirement in the US is that a financial institution must file electronically a Currency Transaction Report or CTR for each transaction that exceeds $10,000 whether it is

money coming into or out of the entity. Transactions of certain persons, however, are exempt from being reported.

Federal regulations require the filing of an SAR on four occasions: criminal violations involving insider abuse for any amount; criminal violations in excess of $5,000 for an identified suspect; criminal violations in excess of $25,000 regardless of a potential suspect; and transactions conducted or attempted in excess of $5,000, if suspected that the transaction is for money laundering or terrorist financing. In addition, if the financial institution cannot explain the purpose of the transaction when it's outside the normal course of business for that customer, then it should also be reported. In cases where the suspicious transaction is a cash transaction exceeding the CTR threshold, both the STR and CTR can be filed.

In the EU there is a threshold of €10,000 for cash transactions but this relates to occasional transactions in order for the financial institution to request full KYC documentation and perform CDD procedures.

3.5 Implementation of KYC standards in a cross-border context

The FATF and other standard-setting bodies, such as Basel and the European Union, require that firms take specific measures to comply with KYC and CDD requirements, where they have operations in more than one jurisdiction.

Supervisors around the world should seek, to the best of their efforts, to develop and implement their national KYC standards fully in line with international standards so as to (1) avoid potential regulatory arbitrage and (2) safeguard the integrity of domestic and international banking systems. The implementation and assessment of such standards put to the test the willingness of supervisors to cooperate with each other in a very practical way, as well as the ability of banks to control risks on a group-wide basis. This is a challenging task for firms and their supervisors.

The supervision of international companies can only be effectively carried out on a consolidated basis, and reputational risk as well as other types of risks are not limited to national boundaries. Parent companies must communicate their policies and procedures to their overseas branches and subsidiaries, including trust companies, and have a routine for testing compliance against both home and host country KYC standards in order for their programs to operate effectively globally. Such compliance tests will also be tested by external auditors and supervisors. Therefore, it is important that KYC documentation is properly filed and available for inspection. As far as compliance checks are concerned, supervisors and external auditors should in most cases examine systems and controls and look at customer accounts and transactions monitoring as part of a sampling process.

However small an overseas establishment is, a senior officer should be designated to be directly responsible for ensuring that all relevant staff are trained in, and observe, KYC procedures that meet both home and host standards. While this officer will bear primary responsibility, he should be supported by internal auditors and compliance officers from both local and head offices as appropriate.

Where the minimum KYC standards of the home and host countries differ, branches and subsidiaries in the host jurisdictions should apply the higher standard of the two. In general, there should be no impediment to prevent a firm from adopting standards that are higher than the minimum required locally. If, however, local laws and regulations (especially secrecy provisions) prohibit the implementation of home country KYC standards, where the latter are more stringent, host country supervisors should use their best endeavours to have the law and regulations changed. In the meantime, overseas branches and subsidiaries would have to comply with host country standards, but they should make sure the head office or parent company and its home country supervisor are fully informed of the nature of the difference.

Criminal elements are likely to be drawn toward jurisdictions with such impediments. Hence, firms should be aware of the high reputational risk of conducting business in these jurisdictions. Parent companies should have a procedure for reviewing the vulnerability of the individual operating units and implement additional safeguards where appropriate. In extreme cases, supervisors should consider placing additional controls on firms operating in those jurisdictions and ultimately perhaps encouraging their withdrawal.

During on-site inspections, home country supervisors or auditors should face no impediments in verifying the unit's compliance with KYC policies and procedures. This will require a review of customer files and some random sampling of accounts. Home country supervisors should have access to information on sampled individual customer accounts to the extent necessary to enable a proper evaluation of the application of KYC standards and an assessment of risk management practices and should not be impeded by local secrecy laws.

In certain cases, there may be a serious conflict between the KYC policies of a parent company imposed by its home authority and what is permitted in a cross-border office. There may, for example, be local laws that prevent inspections by the parent companies' compliance officers, internal auditors, or home country supervisors, or that enable customers to use fictitious names or to hide behind agents or intermediaries that are forbidden from revealing who their clients are. In such cases, the home supervisor should communicate with the host supervisor in order to confirm whether there are indeed genuine legal impediments and whether they apply extraterritorially.

If they prove to be too great to be overcome and there are no satisfactory alternative arrangements, the home supervisor should make it clear to the host that the firm may decide for itself, or be required by its home supervisor, to close down the operation in question.

In the final analysis, any arrangements underpinning such on-site examinations should provide a mechanism that permits an assessment that is satisfactory to the home supervisor. Statements of cooperation or memoranda of understanding setting out the mechanics of the arrangements between home and host supervisors may be helpful. Access to information by home country supervisors should be as unrestricted as possible, and at a minimum they should have free access to the firms' general policies and procedures for customer due diligence and for dealing with suspicions.

4. Learning summary

- CDD includes, identification, verification of the customer, understand the purpose of the business relationship and monitoring of transactions.
- Simplified Due Diligence (SDD) may be applied where the money laundering and terrorist financing risk is low. SDD measures include adjusting the timing of CDD, adjusting the quantity of information obtained for identification, verification or monitoring purposes, adjusting the frequency of CDD updates and reviews of the business relationship, and adjusting the frequency and intensity of transaction monitoring.
- Enhanced Due Diligence may be applied where the money laundering and terrorist financing risk is higher than the acceptable. EDD measures that firms can apply may include increasing the quantity of information obtained for CDD purposes, increasing the quality of information obtained for CDD purposes to confirm the customer's or beneficial owner's identity and increasing the frequency of reviews to be satisfied that the firm continues to be able to manage the risk associated with the individual business relationship.
- Enhanced Due Diligence must always be applied when dealing with PEPs, persons with personal links in high-risk third countries, in correspondent banking relationships with a third-country respondent institution and when a customer performs unusual or complex transactions.
- Automated screening and monitoring systems can issue alerts and allow the entity to perform additional checks on specific customers or transactions.
- For regulated entities operating cross-border, they need to ensure that there are appropriate procedures in place to ensure compliance with the policies of the parent company.

5. End of Chapter Questions

Think of an answer for each question and refer to the chapter content for confirmation.

- ✓ When is KYC and CDD applied?
- ✓ What are the elements of CDD?
- ✓ What measures should an obliged entity apply when conducting SDD?
- ✓ What additional measures should an obliged entity apply when conducting EDD?
- ✓ How long should customer information be retained?
- ✓ What is the process of reporting suspicious transactions?
- ✓ What are the measures should an obliged entity apply to ensure compliance of majority-owned companies or subsidiaries operating cross border?

NOTES

Chapter 6

SANCTIONS

Learning Objectives

- Become aware of both the definition and purpose of sanctions.
- Comprehend the difference between the different forms of sanctions (unilateral vs. multilateral), the categories (comprehensive vs. smart and primary vs. secondary).
- Understand why the US, in particular, has made extensive use of secondary sanctions.
- Assess the conditions that will make sanctions successful.
- Comprehend the difference between decisions taken multilaterally and unilaterally
- Understand the decision-making framework for two key international institutions (the EU and the UN)
- See in practical terms if and how these institutions have practically made use of sanctions against Russia in response to the situation in Crimea since 2014.
- Review the limitations of the two international organisations in deciding the use of sanctions
- Analysis of the US case as the sovereign state that has decided unilaterally on imposing sanctions that also include the use of secondary sanctions
- Examine if and how the US can pressure other countries to adopt its sanctions policy

Introduction

International Economic Sanctions have become a central instrument in global governance over the past decades, employed by both sovereign states and international organisations. More recently, there has been a shift towards 'smart' or targeted sanctions that aim for the political and economic elites of targeted countries (e.g. through asset freezes and travel bans) rather than a more comprehensive sanctions approach (e.g. large-scale trade embargoes) that has detrimental effects on civilian populations as well.

In the era of financial globalisation such 'smart' sanctions entail increased compliance obligations both for state institutions and private organisations which, if not met, carry significant fines and penalties. Even more, the US decision to implement secondary sanctions that have an extraterritorial effect, have made sanctions compliance an even more complex and difficult challenge for businesses with a global outreach.

1. Understanding Sanctions

1.1 Key Definitions

Sanctions are considered a coercive foreign policy tool (not involving the use of military force) whereby one party (either an international organisation or a state) disrupts its normal relations with another party, in order to achieve one of the following objectives:

- Induce the targeted state to change its behaviour.
- Generate popular pressure on the government that causes it to change its policies.
- Provide a coup or revolt that leads to the emergence of a new government that will act in accordance with the sanctioning state's wishes.

1.2 Forms of Sanctions

There are two forms of sanctions that need to be clarified:

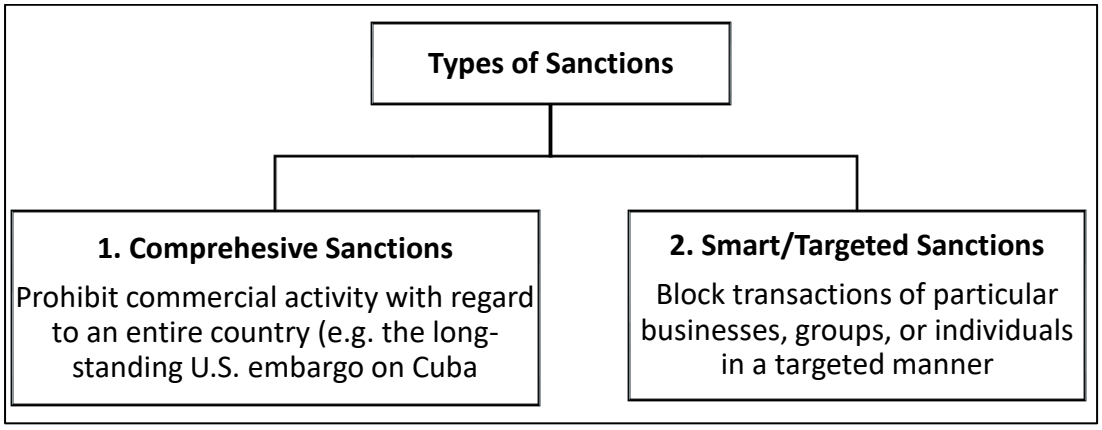
***Unilateral sanctions*:** They involve one country acting independently and enforcing a sanctions policy without securing similar action against the specified target by other parties. An example is the US sanctions on Cuba.

***Multilateral sanctions*:** They involve two or more countries acting in coordination and enforcing a sanctions policy on a specified target. This may involve international organisations as well (Example: UN sanctions on Democratic People's Republic of Korea)

1.3 Categories of Sanctions

Furthermore, whether imposed unilaterally or multilaterally sanctions can be categorised into two main types of sanctions as illustrated in Figure A below:

Figure A: *Types/Categories of Sanctions*


Types of Sanctions
1. Comprehesive Sanctions
Prohibit commercial activity with regard to an entire country (e.g. the long-standing U.S. embargo on Cuba
2. Smart/Targeted Sanctions
Block transactions of particular businesses, groups, or individuals in a targeted manner

Comprehensive Sanctions

The traditional *comprehensive approach* to sanctions involves a broader application of restrictive measures on the targeted country. As a result of the hardship inflicted on the country and its civilian population, it is expected that grassroot political pressure will be directed on the political establishment and, consequently, there will be a change in policies/behaviour, for example through a change in government via democratic elections, that will allow for the loosening or even withdrawal of sanctions. The transmission mechanism is rather straightforward and is based on a '*pain-gain*' formula where supposedly the greater the pain inflicted on the target state, the greater and quicker the gain for the sanctioning parties.

In recent years, such an approach has been seldomly applied because of the significant practical limitations it has. Effectively, the consequences of such sanction regimes make their imposition counterproductive. The damage inflicted on innocent civilian populations is one of the major restricting factors. Additionally, this may easily be exploited by the targeted government to argue that the sanctions regime is inhumane and enable government officials to promote a nationalistic sentiment of resistance against the intrusive outsider. Additionally, at the international level, this may lead to sympathy for the targeted state and criticism against the countries/organisations that decide to implement comprehensive sanctions.

Even more, it must be noted that when comprehensive sanctions are imposed on an autocratic state, then the slimmer are the chances of bringing about a change since civilian 'pain' cannot be translated into votes in a democratic electoral procedure, thus rendering the transmission mechanism ineffective to a great extent.

In an attempt to overcome such limitations, sanctions, as a foreign policy tool, have adjusted accordingly and have become more '*smart*' and '*targeted*'.

Smart Sanctions

Although the end goal might be the same as that of comprehensive sanctions, the revised *smart sanctions* have introduced alternative approaches in securing the effectiveness of the sanctions imposed. The two most important issues that have been reconsidered are:

A. An improvement in the procedures for **humanitarian exemptions**: Smart sanctions aim to protect vulnerable social groups (for example, children, women, and the elderly) from so-called collateral damage (unintended economic and social effects) by exempting specified commodities (such as food and medical supplies) from a possible embargo.
B. **Setting clear, specific and identifiable targets (usually focusing on the political and economic elites)**: Smart sanctions effectively target and penalise the political and economic elites espousing policies and committing actions deemed reprehensible by the international community. Leaders are considered more inclined to comply once their personal economic positions or their inner circle are hit.

Targeting political elites complements the humanitarian exemptions element of a smart sanctions regime. In response, there are three categories of targeting instruments that have been established:

1. arms embargoes;
2. travel restrictions; and
3. financial sanctions (e.g. freezing of foreign bank accounts, seizure of assets and properties and denial of private bank loans) that have become an ever-more popular tool in recent years

1.4 Primary Vs Secondary Sanctions

Having analysed the key categories of sanctions another important distinction between primary and secondary sanctions needs to be clarified.

The conventional sanctions policy option involves two parties where primary sanctions are imposed prohibiting companies and individuals in the sanctioning party from engaging with their counterparts in the sanctioned party.

Importantly, countries may opt for secondary sanctions in addition to primary sanctions. The key distinction between the two is that secondary sanctions may have an indirect effect on countries that neither impose the sanctions nor are the primary target. For example, imagine we have three countries where country A imposes sanctions on country B while country C is neither the sanctioning nor the sanctioned country. Essentially, secondary sanctions by country A will put pressure on the third party (country C) to stop its activities with the sanctioned country (country B) by threatening to cut-off the third party's (country C's) access to the sanctioning country (country A).

Secondary sanctions are alternatively referred to as extraterritorial sanctions where the term '*extraterritoriality*' is the ability of a state to make, apply, and enforce laws, regulations, and other rules of conduct in respect to persons, property, or activity beyond its territory.

The US stands out as the prominent example of a country that makes use of such sanctions. The US secondary sanctions are sanctions that the US can apply to wholly non-US actors in wholly non-US transactions of which the US administration disapproves. For example, US secondary sanctions threaten to cut off non-US persons, such as European businesses, from the US financial system for transactions or certain other dealings with US-targeted actors, such as designated Iranian or Russian businesses or sectors. The US dollar and US financial system provides for the reach of such secondary sanctions.

On the contrary, the EU believes that secondary sanctions constitute a violation of international law and does not allow for extraterritoriality for sanctions. EU sanctions, therefore, apply only to all EU persons worldwide and where links to the EU are present (i.e. they are essentially primary sanctions).

Moreover, in 1996 and in response to US extraterritorial measures concerning Cuba, Iran and Libya, the EU adopted a blocking statute (Regulation (EC) No. 2271/96) whereby EU operators

engaged in lawful international trade and/or movement of capital, as well as related commercial activities, were protected against the effects of the US extra-territorial legislation.

The blocking statute prohibits compliance by EU operators with any requirement or prohibition based on the specified foreign laws. EU operators whose economic and financial interests are affected by the extra-territorial application of those laws are obligated to inform the European Commission.

If EU operators consider that non-compliance with a requirement or prohibition based on the specified foreign laws would seriously damage their interests or the interests of the Union, they can apply to the Commission for an authorisation to comply with those laws. Such an authorisation may be granted by the Commission in specific and duly motivated circumstances, and as a derogation from the rule.

On 6 June 2018, the EU adopted a delegated act amending Regulation (EC) No 2271/96 (the Blocking Statute) in order to counteract the extra-territorial application of certain US sanctions in the EU. This happened in response to the US administration's announcement of its unilateral withdrawal from the Joint Comprehensive Plan of Action (JCPOA) and the re-imposition of the US primary and secondary sanctions on Iran.

Nevertheless, the effectiveness of the EU's Blocking statute has been questioned and it has even been described as a toothless tool until now. Primarily, the Blocking Statute does not contain a direct enforcement and sanction mechanism as these remain under the Member States' authority. It could thus prove somehow controversial for a Member State to sanction a national company for complying with US laws in order to avoid high fines from the US administration and courts.

Under a scenario where the European Commission and the Member States actually display the political commitment and begin to enforce the Blocking Statute rigorously, many companies will have no choice but to be in violation of either EU or US law. Undoubtedly, legal uncertainty will prevail, at least in the short-run, but as the US has a history of strict sanctions enforcement, many companies may consider potential EU fines to be of a lesser worry. This can prove to be a blow to the credibility of the EU's sanctions policy.

1.5 When are sanctions successful?

When is the leverage of the sanctioning party most effective?

Sanctions are more likely to be successful when the following conditions are met:

1. The **pre-sanctions trade volumes** between the involved parties need to be important for economic sanctions to have an effect on the targeted country.
2. Sanctions tend to succeed most in the **initial years of implementation**. The longer sanctions need to be applied for, the greater the adjustment period for the targeted country during which it is given the opportunity to undertake a necessary adjustment process (e.g. a reallocation of resources within its economy) that will allow it, at least

to some extent, to deal with the adverse effects resulting from the sanctions imposed. Sanctions should be imposed quickly and decisively to maximize impact.

3. The **Political Regime/System in the Target Country**: If the target state is **democratic** (as opposed to **authoritarian**) this will allow for opposition parties to put forward alternative policy suggestions that can relieve the country from the sanctions regime. In a democratic state the opposition parties will be given the chance to present their alternative strategies in a fair electoral process that may result in a change of government. In contrast, in authoritarian regimes, the opposition parties are usually marginalised, freedom of speech is censored and state propaganda dominates the media. Effectively, this secures a mobilisation of popular support for the governing elite by initiating a patriotic reaction against the 'external threat' that targets the nation's interests through the imposition of sanctions.
4. Strong **multilateral political commitment** makes sanctions more effective. Where a number of states (or, even better, an international organisation such as the UN or the EU) agree on the imposition of sanctions, then the possibility for the targeted state to evade the sanctions becomes limited. A sanction regime imposed by the UN, when compared to unilateral actions by a single state, not only carries international legitimacy but also political clout.
5. **Multiple policy instruments** increase the success rate of sanctions. Sanctions stand a better chance of success when a variety of sanction types is adopted. For example, implementing simultaneously an arms embargo, a travel ban and an asset freeze will certainly enhance the coercion exerted on the target country.
6. The **goal is relatively modest**. By setting the bar low, the chances of success increase even with the imposition of more modest sanctions. On the contrary, when one aims for more ambitious targets that in practice are more difficult to reach, then the reaction by the targeted country may be more confrontational and the use of more tough sanctions will be required (while multilateral cooperation becomes essential).
7. **Size/Power of Target State**: The chances of success increase when the target is much smaller than the country imposing sanctions, economically weak, and politically unstable. A large country that is economically strong and has an established political leadership that faces little challenge is bound to better manage the imposition of sanctions.
8. **Effects on Sender/Sanctioning State**: The Sender State should avoid high economic or political costs to itself ('boomerang effect'). This may prove to be a complex and tricky requirement, since the greater the financial and commercial interdependence between the related parties, the harder the effects on the targeted country will be. Therefore, it must be secured that the country imposing the sanctions can manage the adverse effects stemming from the implementation of sanctions.

The ending of unsuccessful sanctions may prove to be a difficult task for the party imposing the sanctions. If the sanctions are unsuccessful in changing or containing the targeted behaviour, then there is no justification to end the sanctions and thus the party imposing the

sanctions may be dragged in an open-ended and costly situation that needs to be sustained in order not to lose face. A possible way out may be a change in government (or leadership) in either of the parties involved that may give room for a reassessment of the sanction regime and a reconciliation of the whole situation through compromise, while shifting blame (and political cost) to previous administrations.

The operational framework for sanctions policy may differ according to the organisation or state that decides, and it is important to distinguish between the various decision-making fora. In doing so, special emphasis is placed on the two most prominent **international organisations** (the **United Nations** and the **European Union**) while in reviewing **unilateral sanctions** the case of the **United States (US)** is analysed, given that the US has the leverage to impose sanctions in a unilateral manner and, in practice, has used economic and financial sanctions more than any other country.

2. Sanction Lists

2.1 United Nations Sanctions

The United Nations (UN) is an international organisation founded in 1945. It is currently made up of 193 Member States.

The mission and work of the United Nations are guided by the purposes and principles contained in its founding Charter. Within the Charter there is specific reference to Sanctions. Specifically, under Chapter VII (*Actions with respect to threats to the peace, breaches of the peace, and acts of aggression*) there is Article 41 which notes the following:

The Security Council may decide what measures not involving the use of armed force are to be employed to give effect to its decisions, and it may call upon the Members of the United Nations to apply such measures. These may include complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communication, and the severance of diplomatic relations. (Link)

The Security Council mentioned in Article 41 is one of the two principal organs of the UN that have the authority to pass resolutions. The other is the General Assembly. Nevertheless, there is a significant difference between the two organs with reference to sanctions policy. On the one hand, the **General Assembly** (composed of every UN member state) has the authority to pass **legally non-binding** resolutions that offer recommendations for UN member states to adopt economic sanctions. Interestingly, in relation to developments in Crimea in 2014 the General Assembly did pass a relevant Resolution by majority, essentially dismissing the annexation of Crimea by Russia as illegal.

The UN General Assembly Resolution regarding Ukraine - Resolution 68/262 Territorial integrity of Ukraine (Link)
The annexation of Crimea was dismissed by the General Assembly as illegal. The official text of the relevant Resolution does not identify Russia by name but describes the referendum that took place in Crimea as "having no validity" and calls on countries not to recognize the redrawing of Ukraine's borders. (Voting in the General Assembly: 100 in favour, 11 votes against and 58 abstentions). The US and the EU lobbied intensely for its passage since it was considered an important pressure point on Russia. The Resolution has no enforcement power and mostly carries a symbolic value without necessarily having any practical effect. All great powers (including the US and Russia) have in previous occasions ignored similar resolutions.

On the other hand, the **Security Council** (consisting of 15 member states whereby 5 are permanent members - including USA, Russia, UK, France and China - and 10 serve rotating terms of two years each) has the authority to pass **both legally non-binding 'recommendations' and binding 'decisions' for UN member states to impose sanctions**.

That being said, it is important to note that decisions reached within the Security Council are taken in a complex manner and have certain particular characteristics. Most importantly, all permanent members have the right to veto any decision within the Security Council. Thus, effectively, one would never expect to see the Security Council taking any sort of decision targeting one of the permanent member states. In addition, decisions are the result of a political bargaining process among the very diverse and conflicting political interests represented in the Security Council. This may lead to a political compromise between, on the one hand, states wanting to be tough on violators of international norms of good behaviour and, on the other hand, states wanting only symbolic—and ultimately ineffective—acts; thus, the texts of the resolutions tend to become watered down in order to be accepted by all.

Nevertheless, even within this sensitive decision-making framework, the Security Council has applied sanctions in order to support peaceful transitions, deter non-constitutional changes, constrain terrorism, protect human rights and promote non-proliferation (for example the cases of Somalia, Liberia, and Yugoslavia in the 1990s). But despite cases of cooperation, sanctions remain a divisive issue. For instance, since 2011, Russia and China have vetoed several Security Council resolutions concerning the conflict in Syria, some of which could have led to sanctions against President Bashar al-Assad's regime.

2.2 The European Union Sanctions

The European Union is a unique economic and political union between 27 EU countries that together cover much of the continent. As part of the European integration process, a significant number of policies are now decided at the European level, within well-defined

policy-making procedures that only in certain cases require unanimity by the member states (mostly in relation to foreign policy, defence and security and fiscal policy).

'*Sanctions*' or **'*restrictive measures*'** are an essential tool of the EU's Common Foreign and Security Policy (CFSP). They are used by the EU as *part of an integrated and comprehensive policy approach*, involving political dialogue, complementary efforts and the use of other instruments at its disposal. Importantly, decisions on sanctions taken at the European level still require unanimity by EU Member States. EU member states then, at the national level, adopt their own legislation for monitoring and enforcing decisions on sanctions.

The European Union's Sanction Policy: The EU can impose restrictive measures either on its own initiative or in order to implement UN Security Council resolutions. Specifically, the EU implements all sanctions adopted by the UN Security Council and is involved in a permanent dialogue with the UN to better coordinate EU member states' respective actions on sanctions. Additionally, the EU may also reinforce UN sanctions by applying measures in addition to those imposed by the UN Security Council (in what is called a mixed sanctions regimes). Finally, the EU can autonomously decide on sanctions.

The **objectives of the EU** are based on the following points:

- safeguarding EU's values, fundamental interests, and security
- preserving peace
- consolidating and supporting democracy, the rule of law, human rights and the principles of international law
- preventing conflicts and strengthening international security

It is also of great importance for the EU to avoid Collateral Damage when deciding on sanctions. Sanctions are developed in such a way as to minimise adverse consequences for those not responsible for the policies or actions leading to the adoption of sanctions. In particular, the EU works to minimise the effects on the local civilian population and on legitimate activities in or with the country concerned.

EU sanctions seek to bring about change in the policy or conduct of those targeted, with a view to promoting the objectives of the EU's CFSP. Possible targets include:

- governments of non-EU countries because of their policies
- entities (companies) providing the means to conduct the targeted policies
- groups or organisations such as terrorist groups
- individuals supporting the targeted policies, involved in terrorist activities, etc

Each regulation on sanctions lays down the precise scope of the measures and details for their implementation. As a legal act of general application, the regulation is binding on any person or entity (economic operators, public authorities, etc.) within the EU. Specifically, EU sanctions apply:

- within the jurisdiction (territory) of the EU;

- to EU nationals in any location;
- to companies and organisations incorporated under the law of a member state - including branches of EU companies in third countries;
- on board of aircrafts or vessels under member states´ jurisdiction.

The EU Sanctions in response to Russian involvement in the Ukrainian Crisis

The EU has adopted a broad sanction regime targeting Russia in response to the country's involvement in the Ukraine crisis in 2014, during which Russia annexed the Crimea region of Ukraine. This regime was introduced in **three phases**, each one intending to further increase the pressure on Russia and since then, the sanctions have been renewed and will continue to be, until Russia fully implements the terms of the Minsk peace agreements (February 2015) or some other compromise is reached. The terms of the Minsk agreements include an immediate and full ceasefire, the return of all hostages and illegally held people, and the restoration of Ukrainian control over the Crimea region[5].

Analytically, the three steps shaping the EU sanction regime on this issue are:

Step 1: EU Sanctions Targeting Russia (17 March 2014) – Targeting Individuals/ Entities

1. **Council Decision 2014/145/CFSP** (Link)
2. **Council Regulation (EU) No 269/2014** (Link)

Concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine.

In summary:

- EU imposed asset freezes and travel bans against Russian and Ukrainian officials and strongly condemned the unprovoked Russia violation of Ukraine's sovereignty;
- EU cancelled bilateral summits with Russia and most EU programmes involving Russia, with the exception of civil society and cross-border cooperation;
- Froze assets of persons and entities in the EU (the list will continue to grow as the sanctions are strengthened reaching 155 people and 44 entities) The updated list is available through this link

[5] At a summit in Minsk on 11 February 2015, the leaders of Ukraine, Russia, France, and Germany agreed to a package of measures to alleviate the ongoing war in eastern Ukraine. The implementation of the provisions of the Agreement is still pending.
Key provisions included:

- a ceasefire starting on 15 February
- withdrawal of heavy weapons beginning on 17 February, and completed within two weeks; all prisoners to be released, with amnesties for those involved in the fighting;
- withdrawal of all foreign-armed formations, weapons and mercenaries from Ukrainian territory, as well as disarmament of all illegal groups;
- constitutional reform to enable decentralisation of the rebel regions by the end of 2015 and restoration of Ukrainian border controls with Russia, to be completed by the end of 2015.

- The EU outlawed trade with and investment in Crimea and banned EU operators from tourism activities in Crimea.

The Council has renewed this decision every six months

Step 2: EU Sanctions against Russia (24 June 2014) – Targeting Crimea area

1. **Council Decision 2014/386/CFSP** (Link)
2. **Council Regulation (EU) 692/2014** (Link)

Concerning restrictions on goods originating from Crimea or Sevastopol, in response to the illegal annexation of Crimea and Sevastopol

The Council adopted measures to implement the EU's policy of non-recognition of the illegal annexation of Crimea and decided on a ban on goods originating from Crimea or Sevastopol. EU banned EU individuals and EU-based companies from importing goods, exporting certain goods and technologies, and providing tourism services in Ukraine's Crimea region. The EU also has restricted trade and investment in certain economic sectors and infrastructure projects.

The Council has renewed this decision annually

Step 3: EU Sanctions against Russia (31 July 14) – Introducing Sectoral Sanctions

1. **Council Decision 2014/512/CFSP** (Link)
2. **Council Regulation (EU) 833/2014** (Link)

Concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine

EU imposed economic sanctions targeting exchanges with Russia in specific economic sectors.

Sectoral Sanctions:

- Restricting Russia's access to EU capital markets: EU nationals and companies may no more buy or sell new bonds, equity or similar financial instruments with a maturity exceeding 90 days, issued by major state-owned Russian banks, development banks, their subsidiaries outside the EU and those acting on their behalf. Services related to the issuing of such financial instruments, e.g. brokering, are also prohibited;
- Embargo on the import and export of arms and related material from/to Russia;
- Agreement on a prohibition on exports of dual use goods and technology for military use in Russia or to Russian military end-users;
- Exports of certain energy-related equipment and technology to Russia will be subject to prior authorisation by competent authorities of Member States.

Effects: far-reaching impact on Russia's economy and EU-Russia economic relations. These sanctions limited access to EU markets for Russian state-owned financial institutions, instituted an embargo on the arms trade, and a ban on imports and exports of sensitive technologies.

The Council has renewed this decision every six months

The Consolidated list of persons, groups and entities subject to EU financial sanctions **(Link)**

In order to facilitate the application of financial sanctions, the European Banking Federation, the European Savings Banks Group, the European Association of Co-operative Banks, the European Association of Public Banks ("the EU Credit Sector Federations") and the European Commission recognised the need for an EU consolidated list of persons, groups and entities subject to financial sanctions and more precisely the freezing of assets. The Credit Sector Federations set up an initial database containing the consolidated list. The European Commission subsequently took over this database and is responsible for its maintenance and for keeping the consolidated list of sanctions up-to-date.

The consolidated list of persons, groups and entities subject to EU financial sanctions can be downloaded from ***Financial Sanctions Database - FSF platform*** accessible via the following address: https://webgate.ec.europa.eu/europeaid/fsd/fsf

In order to access the FSF platform you need to have an "EU Login" account. The instructions provided on the EU Login page displayed when you click on the above link are straightforward and easy to follow.

2.3 Unilateral Sanctions: The case of the US

As discussed previously, multilateral sanctions involve two or more countries deciding together to impose a sanctions regime. Alternatively, there is also the scenario where countries may unilaterally decide and apply sanctions. Any sovereign state is entitled to determine its foreign policy and impose sanctions against other parties where it deems these to be appropriate and beneficial for its national interests.

Nevertheless, imposing sanctions unilaterally is considered a high-risk foreign policy option since, without multilateral support from other countries, the prospect of delivering the desired result is rather dim. On the contrary, the larger the number of countries involved, the greater the leverage against the targeted country.

The US, given its unique global role and power, has often unilaterally pursued and applied economic and financial sanctions as part of its foreign policy. The financial might of the US and the influence it can exert in the international economic arena, enable the country, if it so decides, to formulate its sanctions policy in a credible (although not necessarily successful) manner, even without having *a priori* secured the cooperation of other countries.

For example, on the current financial sanctions' regime imposed on Russia, the US has played a leading role and at times has done so without any prior communication with its traditional western allies.

Given the influential role of the US in shaping the sanction regime against Russia, this section will look into the following:

- Why does the US issue sanctions unilaterally?
- Which are the relevant institutions with decision-making powers?
  - Can the President of the US decide on his/her own?
  - Can any branch of government (executive, legislative or judiciary) decide unilaterally?
- How can the US pressure other countries to adopt its sanctions policy?
- What are the most significant developments in the US sanctions policy framework? What is the global outreach of these developments?
- Has the US made use of secondary sanctions and what can be the consequences/effects of such a policy?

2.4 Why does the US issue sanctions unilaterally?

The US has enjoyed a primacy in the international financial system, given the pivotal role of the dollar. Even more, no other currency (including the euro), at the moment, can pose a credible alternative that may replace the dollar as a unique currency of global importance. The absence of viable alternatives strengthens the dollar's durability and increases the leverage of the US relative to other countries.

Recent data notes that the US accounts for about 20 percent of the world's economic output, while more than half of all global currency reserves and trade are in dollars (Bloomberg, 2018). Even more, according to the IMF, the dollar still represents roughly 62 percent of all sovereign reserves, with the euro at 20 percent.

Importantly, as part of its sanctions policy the US has also adopted secondary sanctions whereby foreign corporations, financial institutions and individuals can be refrained from doing business with US-sanctioned entities given that the US has the necessary nexus (either through a US bank or the American payments system) to prosecute the offender or act against its American assets. This gives the US extraterritorial reach over non-Americans trading with or financing a sanctioned party. The mere threat of prosecution can destabilize finances, trade and currency markets, effectively disrupting the activities of non-Americans.

In better understanding/explaining the US sanctions policy and how this has developed, one must also review the institutional framework within which decisions are taken at the national level. Does the political system of the US (including the relevant institutional framework) allow the President (Head of the Executive) to carry out such policies independently and how can the other branches of Government intervene and shape the policies differently? Furthermore, which department is responsible for executing sanctions policies and, finally, who can actually

initiate a change in sanction policies? In dealing with these questions, the following sections allow for a clearer understanding as to how sanctions are decided by the US

2.5 US Decision-Making Framework

The Constitution is clear in entrusting the Congress (the Legislative Branch) with the power to "regulate commerce with foreign nations" while at the same time it provides no power to the President (the Executive Branch) to impose sanctions or to refuse to implement congressionally mandated sanctions.

Nevertheless, the Congress allowed for sanction policies to be transferred under the authority of the POTUS, possibly acknowledging the benefits of allowing the President to respond to national threats through coercive economic diplomacy. The International Emergency Economic Powers Act (IEEPA) of 1977 practically handed to the President unlimited discretion to impose sanctions for national security purposes, in wartime and peacetime alike.

(IEEPA) (1977) (Link) is key in understanding how the President may act and decide on sanctions and the following provisions enable to better understand how the US sanctions policy is shaped and decided:

- IEEPA enables the Executive to protect the country from **national security threats**, involving the Department of the Treasury in a leadership capacity.
- IEEPA authorizes the U.S. Presidents to **regulate commerce** (including the power to investigate, regulate, and block transactions) after *"any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States."*. What exactly constitutes "unusual" or "extraordinary" is not explicitly defined.
- The President has **complete discretion** in declaring a **national emergency** under IEEPA. IEEPA provides that "[t]he authorities granted to the President . . . may not be exercised for any other purpose," and further, that "[a]ny exercise of such authorities to deal with any new threat shall be based on a new declaration of national emergency."
- Provided that the President first declares a national emergency the President may invoke the authorities granted to his office in IEEPA to investigate, regulate, or prohibit transactions in foreign exchange, use of U.S. banking instruments, the import or export of currency or securities, and transactions involving property or interests in property under U.S. jurisdiction.
- For an emergency declared under the Act to remain in effect, it must be renewed annually.
- Following the POTUS's declaration of a state of national emergency, it is the Treasury Department's Office of Foreign Asset Control (OFAC) that is responsible for maintaining lists of designated individuals and companies, as well as, implementing

regulations and enforcing violations. Running afoul of sanctions may incur regulatory penalties such as fines, but there are also criminal penalties for violating IEEPA.

- IEEPA, through its reporting requirements, provides for **congressional oversight** over the Office of Foreign Asset Control (OFAC) for the duration of the declared national emergency. IEEPA requires that the President immediately transmits to Congress a report specifying his/her actions taken under IEEPA and the reasons for taking such actions, and updates Congress on this information at least once every six months.
- Actions taken under IEEPA are subject to judicial review, an ex-post safeguard.

Since its passage, presidents have relied on IEEPA to enact financial and economic sanctions against a host of countries, including Iran, North Korea, Syria, South Sudan, Russia, and Cuba to name a few, for threats ranging from terrorism and narcotics trafficking to human rights violations and WMD proliferation.

***What is an Executive Order*?**

- It is a written order issued by the President to the federal government which does not require congressional approval.
- Executive orders may prove to be controversial because they bypass approval from Congress, allowing the president to act on his own.
- With an executive order, the President instructs the government how to work within the parameters already set by Congress and the Constitution. In effect, this allows the President to push through policy changes without going through Congress.
- By issuing an executive order, the president does not create a new law or appropriate any funds from the U.S. Treasury; only Congress has the power to do both of these things.
- Legal Base of the EO: the Constitution states that as head of the executive branch and commander in chief of the armed forces, the president "shall take Care that the Laws be faithfully executed."

Within the described legal framework, US Presidents have typically launched the process of imposing sanctions by issuing an executive order (EO) that declares a national emergency in response to an "unusual and extraordinary" foreign threat, such as "the proliferation of nuclear, biological, and chemical weapons" (EO 12938). This affords the President special powers (pursuant to the IEEPA) to regulate commerce with regard to that threat for a period of one year, unless extended by him/her or terminated by a joint resolution of Congress (Executive Orders may also modify sanctions). In relation to the developments in Ukraine and the annexation of Crimea by Russia, the Obama Administration issued in total four Executive Orders as the actions of Russia against Ukraine were considered to be a source of national threat by the US administration.

Analytically the four Executive Orders are the following:

E.O. 13660 – Blocking Property of Certain Persons Contributing to the Situation in Ukraine (6 March 2014)

US - Executive Order 13660 by **President Obama** (Link)

The E.O. *authorizes the* ***Secretary of the Treasury***, in consultation with the Secretary of State, *to* ***impose sanctions*** on those determined to be undermining democratic processes and institutions in Ukraine or threatening the peace, security, stability, sovereignty, and territorial integrity of Ukraine. Efforts to impose a cost on Russia and those responsible for the situation in Crimea were to be initiated.

E.O. 13661 – Blocking Property of Additional Persons Contributing to the Situation in Ukraine (16 March 2014)

US – Executive Order 13661 (expands upon E.O. 13660) by **President Obama** (Link)

The E.O. issued under the national emergency with respect to Ukraine, concluded that the actions and policies of the Russian government with respect to Ukraine – including through the deployment of Russian military forces in the Crimea region of Ukraine – undermine democratic processes and institutions in Ukraine; threaten its peace, security, stability, sovereignty, and territorial integrity; and contribute to the misappropriation of its assets.

The actions of the US authorities aimed to serve as a notice to Russia that unless it abides by its international obligations and returns its military forces to their original bases and respects Ukraine's sovereignty and territorial integrity, the *United States are prepared to take additional steps to impose further political and economic costs* (via sanctions).

E.O. 13662 – Blocking Property of Additional Persons Contributing to the Situation in Ukraine (20 March 2014)

US – Executive Order 13662 by **President Obama** (Link)

The E.O. further expanded the scope of the national emergency declared in Executive Order 13660 of (6 March 2014), and expanded by Executive Order 13661 of (16 March 2014), finding that the actions and policies of the Government of the Russian Federation, including its purported annexation of Crimea and its use of force in Ukraine, continue to undermine democratic processes and institutions in Ukraine; threaten its peace, security, stability, sovereignty, and territorial integrity; and contribute to the misappropriation of its assets, and thereby constitute an unusual and extraordinary threat to the national security and foreign policy of the United States.

E.O. 13685 – Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to the Crimea Region of Ukraine (19 December 2014)

US – Executive Order 13685 by **President Obama** (Link)

The E.O.:

- prohibits the export of goods, technology, or services to Crimea and prohibits the import of goods, technology, or services from Crimea, as well as new investments in Crimea;
- authorizes the Secretary of the Treasury to impose sanctions on individuals and entities operating in Crimea;
- is intended to provide clarity to U.S. corporations doing business in the region and reaffirms that the United States will not accept Russia's occupation and attempted annexation of Crimea.

President Obama called again on Russia to end its occupation and attempted annexation of Crimea, cease its support to separatists in eastern Ukraine, and fulfil its commitments under the Minsk agreements

Moreover, Russian interests were further targeted via additional Executive Orders that were decided in Response to Cyber-Related activities and Elections Interference. During the Obama Administration there were two such E.O. issues (the second one following the elections that took place in November 2016 but before President Trump officially took over office) and a third one was issued by the Trump Administration.

E.O. 13694 – Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (1 April 15)

US Executive Order 13694 by President Obama (Link)

The Executive Order authorized the Secretary of the Treasury "to impose sanctions on individuals or entities that engage in malicious cyber-enabled activities that create a significant threat to the national security, foreign policy, or economic health or financial stability of the United States."

It granted the Department of Treasury's Office of Foreign Assets Control (OFAC) sweeping authority to designate persons determined, in consultation with the Attorney General and the State Department, to have engaged in certain malicious cyber activities.

E.O. 13757 – Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities (29 December 2016)

US Executive Order 13757 by President Obama (Amendment to Executive Order 13694) (Link)

Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities (Provides additional authority for responding to certain

cyber activity that seeks to interfere with or undermine the election processes and institutions, or those of US allies or partners);

President Obama issued this EO almost three months after the Department of Homeland Security and the Office of the Director of National Intelligence (ODNI) issued a joint statement on 7 October 2016, which said that the US intelligence community was "confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organisations" and that "these thefts and disclosures are intended to interfere with the US election process."

E.O. 13848 – Imposing Certain Sanctions in the Event of Foreign Interference in a United States Election (12 September 2018)

US Executive Order 13848 by President Trump (Link)

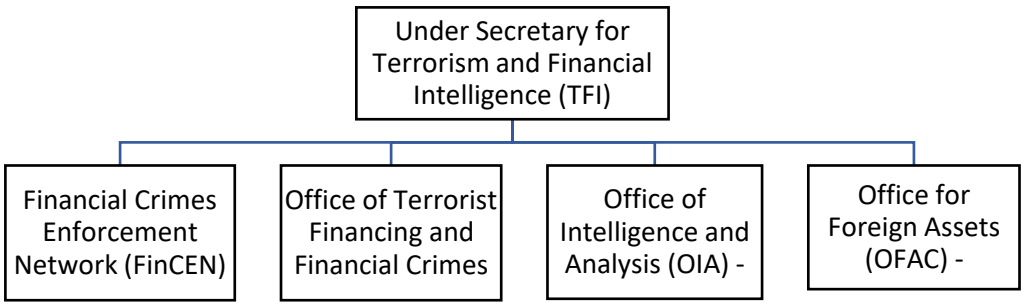
President Trump signed an executive order imposing sanctions on any nation or individual who authorizes, directs, or sponsors meddling operations in US elections. The order would allow for the freezing of assets and the limiting of foreign access to US financial institutions, as well as a cut off of US investment in the sanctioned companies.

2.6 Administration of Sanctions Programme – Who executes the President's decisions?

The administration and implementation of sanctions rests within the U.S. Department of the Treasury whose mission is to (1) maintain a strong economy and create economic and job opportunities by promoting the conditions that enable economic growth and stability at home and abroad, (2) strengthen national security by combating threats and protecting the integrity of the financial system, and (3) manage the U.S. Government's finances and resources effectively.

Headed by an Under Secretary, the Office of Terrorism and Financial Intelligence (TFI) marshals the Treasury Department's policy, enforcement, regulatory, and intelligence functions to sever the lines of financial support to threats to the US national security (international terrorists, WMD proliferators, narcotics traffickers, money launderers, and other)

The structure of the Office for Terrorism and Financial Intelligence is illustrated below:


Under Secretary for Terrorism and Financial Intelligence (TFI)
Financial Crimes Enforcement Network (FinCEN)
Office of Terrorist Financing and Financial Crimes
Office of Intelligence and Analysis (OIA) -
Office for Foreign Assets (OFAC) -

The mandate for the administration and enforcement of economic sanctions is executed by the Office of Foreign Assets Control (OFAC) via the issuing of regulations that direct financial institutions accordingly.

Specifically, OFAC has been assigned certain key duties and responsibilities including the following:

- OFAC administers and enforces economic sanctions imposed on hostile states, nationals and organisations as determined by U.S. foreign policy and national security.
- **Policy Tools**: That mandate is executed by OFAC by issuing regulations that direct financial institutions accordingly.
    - It publishes and updates the **Specially Designated Nationals List** (Link), a comprehensive list of people, organisations, and nations with whom it is prohibited for U.S. Citizens, residents, and organisations to engage in business[6].
    - Although there is no set timetable for updates to the SDN list, OFAC usually releases revisions a few times per month;
    - OFAC may freeze assets and prevent access to the U.S. financial system to enforce its prohibitions, as well as, institute penalties against those who defy its directives;
    - OFAC does not act pursuant to a single set of regulations but rather to particular regulations issued for each sanctions program, each in turn authorized by a separate national-emergency declaration.

Most OFAC designations of Russian individuals and entities have been in response to Russia's 2014 invasion and annexation of Ukraine's Crimea region and Russia's subsequent instigation of separatist conflict in eastern Ukraine.

Sanctions in response to Russia's invasion of Ukraine also consist of sectoral sanctions. Often, sectoral sanctions broadly apply to specific sectors of an economy. In the case of sanctions on Russia, sectoral sanctions have a narrower meaning; they apply to specific entities in Russia's financial, energy, and defence sectors that OFAC has identified for inclusion on the Sectoral Sanctions Identifications (SSI) List. These sectoral sanctions prohibit U.S. individuals and entities from engaging in specific kinds of transactions related to lending, investment, and/or trade with entities on the SSI List, but they permit other transactions.

2.7 OFAC's 50 Per Cent Rule for Entities

Importantly, the OFAC 50 percent rule determines when companies not appearing on the SDN list are considered blocked because they are owned by other companies or people who do appear on the SDN list. The aim of the Rule is to prevent targets from creating complex

[6] *As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and US persons are generally prohibited from dealing with them* (Source: Department of the Treasury)

ownership structures in order to avoid sanctions. Since the August 2014 Revised Guidelines, OFAC notes specifically that:

- '*Property and interests in property of entities directly or indirectly owned 50 percent or more* (not controlled*) in the aggregate by one or more blocked persons are considered blocked regardless of whether such entities appear on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List)*'
- Examples of how the rule applies:
    i. *if Blocked Person X owns 25 percent of Entity A, and Blocked Person Y owns another 25 percent of Entity A, Entity A is considered to be blocked*
    ii. *Blocked Person X owns 50 percent of Entity A, and Entity A owns 50 percent of Entity B. Entity B is considered to be blocked. This is so because Blocked Person X owns, indirectly, 50% of Entity B. In addition, Blocked Person X's 50 percent ownership of Entity A makes Entity A a blocked person. Entity A's 50 percent ownership of Entity B in turn makes Entity B a blocked person*. (Illustration offered below)

Entities A and B are considered blocked and subject to sanction restrictions.

2.8 Other important and relevant agencies in the Executive Branch:

Besides OFAC, there are other agencies in the US executive branch that are relevant with the implementation and administration of other aspects of sanctions policy.

Analytically:

- The **Department of State** restricts visas, arms sales, and foreign aid; implements arms embargos required by the United Nations; prohibits the use of U.S. passports to travel, in limited circumstances; and downgrades or suspends diplomatic relations.
- The Department of Commerce's **Bureau of Industry and Security** (BIS)
    - BIS is within the Department of Commerce. It maintains the Denied Persons List, which is a list of persons for whom export privileges have been denied. The BIS also administers the Export Administration Regulations (EAR). The EAR applies to commodities, technology, software, and other things subject to export controls. A principal goal for the bureau is helping stop proliferation of weapons of mass destruction, while furthering the growth of United States exports. The Bureau is led by the Under Secretary of Commerce for Industry and Security.

- Department of Defense restricts arms sales and other forms of military cooperation.
- Department of Justice investigates and prosecutes violations of sanctions and export laws.

3. Sanctions Compliance Strategy

Any organisation that is exposed to bodies enforcing sanctions needs to be particularly cautious in complying with the sanctions regulatory regime and to avoid any violations that may have legal, financial, reputational, and other adverse consequences.

In better securing an organisation's compliance with requirements stemming from sanctions, an organisation needs to have a sanctions compliance strategy/policy that will clearly set the policy and procedural framework within which the organisation functions. In developing such a policy/strategy, the recommendations of the Wolfsburg Group are a credible reference point.

The Wolfsberg Group has also issued specific **Recommendations** (available on their website) on how best **Sanctions Risk** can be assessed and managed. This Chapter will make extensive reference to the Wolfsberg Group.

Regarding the sanctions regime, Member States should ensure that violation of the national laws transposing the Directive will be punished. Clear rules should be created to empower local authorities to impose these sanctions.

Member states should ensure that at least the breaches related to due diligence, suspicious transactions, record keeping, and internal controls are punished.

The above breaches could be punished with the following means:

- A public statement naming the person or the entity
- An order requiring the cease of the specific activity
- Potential withdrawal of an authorisation
- Temporary ban from certain activities
- Maximum penalty equal to the double of the amount earned from the improper action, or at least €1,000,000

Specifically, for credit institutions, a maximum penalty of €5mln is foreseen, or 10% of its annual turnover. For natural persons (working in credit instructions) the maximum penalty is also €5mln.

FIUs will publish decisions related to the above sanctions when there is no appeal possibility. In some cases, if the publication of the identity is considered disproportional or harmful for the general benefit, FIUs may delay this publication, make it anonymous, or even not make it at all.

For determining the sanctions to be imposed, competent authorities should take into consideration the gravity of the breach, the level of responsibility of the accused person, the financial strength, the derived benefit, the loses of others, the previous breaches by the same people and the potential cooperation with the authorities.

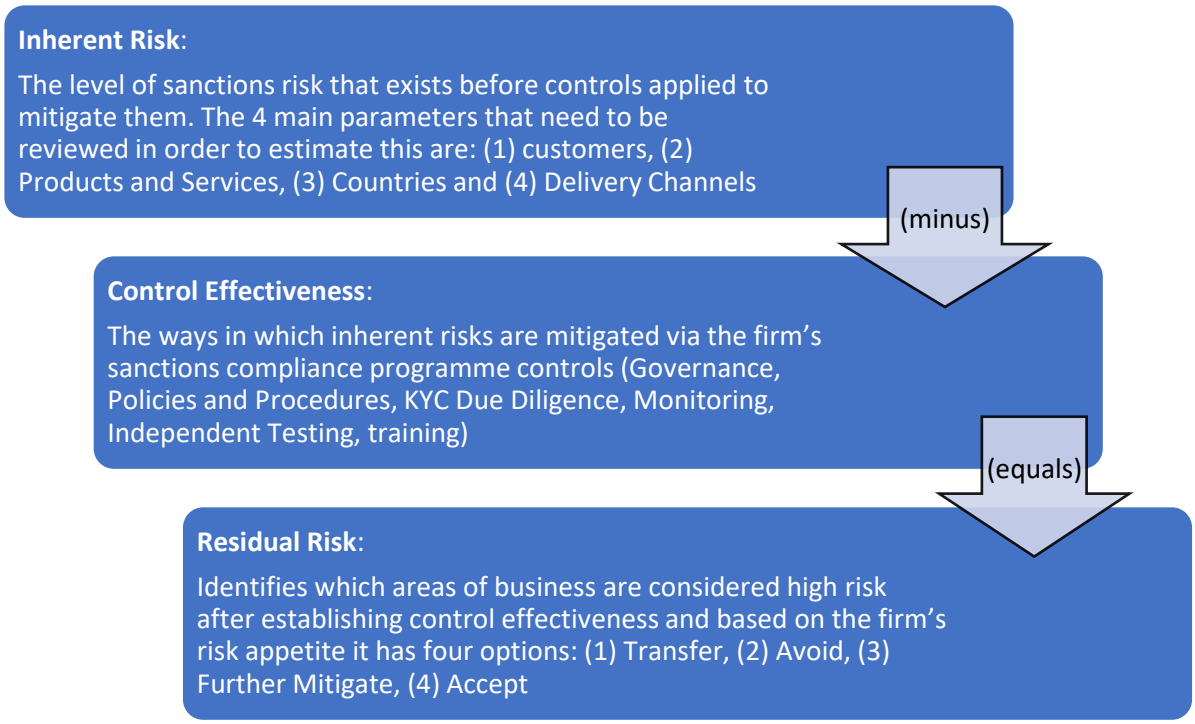
Member states should ensure that people reporting to supervising authorities ("whistle-blowing") are using effective communication channels, follow specifically established procedures and enjoy protection of their personal data. It goes without saying that full confidentiality should exist.

The 4th AML Directive does not dramatically change the Provisions of the 3rd Directive, but it makes certain improvements.

Member states should have transposed it to national law by June 26, 2017.

3.1 Sanctions Risk Assessment

According to the Wolfsberg Group, a three-phased approach can be adopted in order to undertake a risk assessment. Firstly, one needs to determine the Inherent Risk, then, secondly, the effectiveness of the internal controls and the policies in place to mitigate the risk and, thirdly, the residual risk can be identified and dealt with accordingly.


Inherent Risk:
The level of sanctions risk that exists before controls applied to mitigate them. The 4 main parameters that need to be reviewed in order to estimate this are: (1) customers, (2) Products and Services, (3) Countries and (4) Delivery Channels
(minus)
Control Effectiveness:
The ways in which inherent risks are mitigated via the firm's sanctions compliance programme controls (Governance, Policies and Procedures, KYC Due Diligence, Monitoring, Independent Testing, training)
(equals)
Residual Risk:
Identifies which areas of business are considered high risk after establishing control effectiveness and based on the firm's risk appetite it has four options: (1) Transfer, (2) Avoid, (3) Further Mitigate, (4) Accept

Inherent Sanctions Risk

It is important for any organisation to understand the inherent risk it faces before examining how such a risk may be more effectively mitigated.

The Risk Department can be assigned with the duty of thoroughly identifying and assessing the extent to which an organisation may be exposed to sanctions risk. In order for a sanctions compliance program to be effective and credible it must be based on an informed risk assessment that is regularly updated and constitutes the base for the relevant policies and strategies of the organisation.

In order to better identify the extend of the inherent risk an organisation faces it needs to thoroughly review the following four parameters:

- **Identity of the Customer** – Establishing the Ultimate Beneficiary Owner (UBO) and the controlling influences is of critical importance. Many sanctioned individuals are expected to attempt to evade sanctions through incomplete data, complex corporate structures and use of intermediaries. Such an exercise, therefore, needs to focus on the quality of data and 'identifiers', associates of customer, complicated ownership structures, intermediaries, etc.

- **Products and Services** – An organisation needs to be clear as to the extent to which its products or services can be used by the customer in a way that exposes the organisation to the risk of facilitating sanctioned individuals and entities. Products' and services' risk typically arises when a customer misuses a product to evade sanctions, for example with international funds transfers, letters of credit, correspondent banking accounts, and, in particular, payable-through accounts.

- **Country/Geography risk**: The Wolfsberg Group specifically comments that Geography/Country risk is critical in any Sanctions Risk Assessment, not only with respect to sanctioned countries themselves, but also with countries which may have well known/important links or other significant connections to sanctioned countries. These could include countries bordering, or in close proximity to, sanctioned countries, or those countries which present potential opportunities for the diversion of funds with the intent to violate or circumvent sanctions regulations. For instance, on the one hand North Korea stands out as a straightforward example where the country itself is likely to be a red flag but there are other cases of countries that may have political and/or economic relationships with sanctioned countries and may end up being high risk countries. Turkey for instance has boarders with high-risk countries and, consequently, its risk level must be adjusted accordingly. Therefore, it is essential for financial institutions to meticulously identify geographic locations that may pose a higher risk and evaluate the specific risks associated with doing business, opening and servicing accounts, offering products and services and/or facilitating transactions involving certain geographic locations.

- **Delivery channels** are the ways in which products and services are provided by a firm to its customer (also referred to as servicing methods and distribution channels). For example, setting complex delivery channels that rely upon brokers, intermediaries, and other independent third parties, poses a higher sanctions risk than when a business interacts directly with customers and suppliers.

Having determined the inherent sanctions risk an organisation faces, it is then appropriate to see how such a risk may be mitigated.

Mitigating Sanctions Risk

There is a range of actions a business may adopt for a successful Sanctions Compliance Strategy in order to mitigate inherent sanction risks. The most significant are reviewed separately:

- **Management Commitment**. Top-level commitment to an organisation's sanction compliance is essential in order to foster and embed a responsible business culture that highlights the importance of compliance and the need for allocating adequate resources for the purpose of avoiding sanction violations. There must be an explicit tone from the different top levels of the organisation (Board, Executive Management and the entire Management Structure) as they need to lead by example. Towards achieving this target, the following actions are valuable: CEO's active engagement in highlighting the importance of sanctions (via email communication to the staff or through his annual statement), appointing the Chief Compliance Officer as the official in the Executive Committee responsible for sanctions compliance, compulsory targeted training sessions for the Board and Executive Team, allocated time during Board Meetings for briefing and regular sanctions compliance reports presentation by relevant officers)

- Appointing a **Sanctions Compliance Officer:** Such an officer can manage the sanctions compliance strategy and be tasked with control and monitoring responsibilities in relation to sanctions compliance. Such an officer will be the primary point of contact for sanctions compliance and accountable for actions taken in achieving such compliance.

- **Robust and Solid Sanctions Compliance Programme** with clearly defined Policies, Procedures and Internal Controls.

  - <u>Policies and guidance</u>:

    Each organisation must have a clear sanctions policy (published and easily available) in place to set parameters and standards for those working within it, with it and on its behalf. The commitment of the organisation in complying with applicable sanctions must be explicitly outlined in such a document in addition to the following parameters:

      - A breach of sanctions application is strictly forbidden
      - The reasoning behind sanctions compliance is thoroughly explained – stressing the repercussions of non-compliance for the corporation (financial and reputational) but also the disciplinary procedures for company employees should one violate sanctions compliance requirements. The employee is bound to face legal actions that may lead to a fine and imprisonment (depending on the legal framework of the country)
      - Setting at the high level the sanctions compliance controls
      - Highlighting the monitoring and assurance procedures adopted by the corporation and ensuring that this are well understood

  - <u>Compliance manual:</u>

    This manual supports the high-level principles set out in the sanctions policy and needs be tailored to the business, the sector it operates within and the people that

work within it, taking into account a thorough risk assessment carried out within the organisation. The manual must clarify which acts are prohibited, those which require approval and those that are generally safe. It needs to be made clear to the employees working in the first line of defence when, how and by whom to seek help.

- Monitoring of changes to applicable sanctions:

  The organisation needs to set a procedure whereby it follows the decisions/announcements of all the relevant bodies that impose sanctions (whether international organisations or sovereign states) so as to record how the sanctions framework is altered and the adjustments made to the relevant sanctions lists of individuals, entities, sectors and/or geographical areas.

- **Sanctions screening** - Introducing the appropriate Automated Screening Tool (AST) that will be calibrated accordingly to fit the corporation's line of business and undertaken operations.

  According to the Wolfsberg Group, a successful sanctions compliance programme needs to include a screening application. While an organisation could build its own application internally, large organisations will opt for an AST from a vendor. The organisation must take into account its size, geographic presence, operations, range of products offered and technology environment when choosing an AST vendor. There is no "one size fits all" method for implementing an AST, so an institution should analyse its identified sanctions risks and specific operational requirements.

  Per the "*Wolfsberg Guidance on Sanctions Screening*" (Link) an institution needs to consider the following from a risk standpoint:

  - The sophistication and configurability of the matching software
  - Availability of screening rules to optimize alert creation/suppression
  - Support for the screening or transformation of data in non-Latin characters
  - Ad hoc, one-off or manual screening functionality
  - Workflow configurability
  - Availability of metrics reporting

  From a functional standpoint, consideration should be given to the volume of data to be screened; support for multiple local or a single centralized installation; the existence of, or support for, data integrity processes, and the ability of the application to integrate effectively within an organisation's technology infrastructure.

  Regulators emphasize the fact that an automated screening tool should not be treated as something more than tool. ASTs do not completely substitute for a sound understanding about the customer relationship and the expected level of activity and behaviour. Ideally, monitoring should be a combination of both manual and automated screening methods.

- **Audit and Testing** – Assessing the effectiveness of current processes and identifying any inconsistencies between policies and day-to-day operations

➢ Monitoring to assess the functionality of the controls

An organisation needs to ensure that the controls in place function effectively and continue to be sufficient to manage your risk going forward. By a establishing a regular proportionate monitoring comfort is provided to the Board and Executive that the sanctions risk is being effectively mitigated. These monitoring functions will also be reviewed by an investigating regulator if a sanctions breach is alleged or identified

➢ Audit the efficacy of the controls

The efficacy of the controls needs to be regularly audited so as minimise the possibilities of an incident happening as a result of a gap or failure in the sanctions compliance mechanism. An audit system could include:

  - sanction compliance audits – these could focus on reviewing the sanctions compliance policies and processes of the business/operation units and the effectiveness of their practical implementation; also the functioning of the AST
  - internal audit – the internal audit team, though not sanction experts, must be strengthened so as to carry out relevant checks
  - external audit – the sanctions compliance programme should be audited by independent external auditors who can provide an external reassurance for the policies of the organisation

- **Training** – Organisations need to provide focused training that will equip the personnel according to the position held and hold it accountable through assessments. This training should take place on an annual or biennial basis and deliver clear and simple messages to the business about applicable sanctions laws, what this means in practice for them, how to spot potential issues and how to report them within your business.

Residual Risk

Residual risk is the risk that remains after controls are applied to the inherent risk. It is determined by balancing the level of inherent risk with the overall strength of the sanctions compliance strategy and the risk management activities/controls. How each organisation will deal with the residual risk is based on the risk appetite framework that is decided by Board of Directors.

The four basic options businesses have for managing the residual risk are the following:

- Transfer the risk. This is a tricky option since a firm cannot transfer accountability for sanctions compliance to someone else. If a firm assigns responsibility to a vendor or another third party, the firm must ensure the vendor is qualified and has effective controls.
- Avoid the risk. When the level of the residual risk exceeds the firm's risk appetite, then the firm may decide to discontinue or fail to pursue a given line of products, or decide not to accept business relationships with customers who, for example, undertake business in certain countries.
- Further mitigate risk. A firm may choose to introduce additional control mechanisms or strengthen current ones in order to further minimise the residual risk.

- Accept the risk. Given that the residual risk falls within the organisation's risk appetite then this is the expected option.

4. Learning Summary

- Sanctions are considered a coercive foreign policy tool whereby one party (either an international organisation or a state) disrupts its normal relations with another party, in order to achieve specific objectives
- Comprehensive sanctions involve a broader application of specific restrictive measures whereas the more recent alternative approach involves smart sanctions that have specific targets (usually entities and individuals that have close connections with the economic and political elite)
- Primary sanctions involve two parties where one prohibits companies and individuals from engaging with their counterparts in the other party and/or vice versa. Secondary sanctions, however, have an extraterritorial effect as they may affect a third party that neither imposes the sanctions nor is the direct target.
- 'Extraterritoriality' is the ability of a state to make, apply, and enforce laws, regulations, and other rules of conduct in respect to persons, property, or activity beyond its territory.
- While the EU considers that secondary sanctions are a violation of international law, the US is an advent supporter and has made use of them on several instances. The attempt of the EU to introduce measures that countereffect US secondary sanctions has not yet been implemented in a convincing manner.
- A number of conditions needs to be met so that sanctions successfully meet their objectives, otherwise, unsuccessful sanctions may drag on indefinitely since the sanctioning party may wish to pertain a costly situation rather than lose face.
- Two of the most significant international organisations that have the capacity to implement sanctions in a multilateral way are the UN and the EU
- The EU, being a more concise and aligned group of countries (in relation to the UN), has proceeded to adopt targeted measures against Russian interests in relation to developments in Crimea, in contrast to the UN.
- EU sanctions apply:
    - within the jurisdiction (territory) of the EU
    - to EU nationals in any location
    - to companies and organisations incorporated under the law of a member state - including branches of EU companies in third countries
    - on board of aircrafts or vessels under member states´ jurisdiction
- A consolidated list of persons, groups, and entities subject to EU financial sanctions is available and can be downloaded from Financial Sanctions Database - FSF platform.
- The global political and economic status of the US has allowed the country at times to decide unilaterally on the imposition of sanctions and even include secondary sanctions (which have an extraterritorial effect).
- While IEEPA (1977) handed to the US President unlimited discretion to impose sanctions for national security purposes (an authority allocated to the Congress according to the Constitution) recent legal developments (namely the CAATSA Act of 2017) have initiated transferred back authority to the Congress.
- In the implementation of US sanctions, OFAC has a key role to play as it administers and enforces economic sanctions by issuing regulations that direct financial institutions accordingly and in doing so publishes the Specially Designated Nationals List (Link)

5. End of Chapter Questions

Think of an answer for each question and refer to the chapter content for confirmation.

- ✓ Briefly explain the main forms of Sanctions
- ✓ When are sanctions successful?
- ✓ Briefly explain the main sanctions lists
- ✓ What is the US decision making framework with regards to sanctions?
- ✓ What is OFAC's 50 per cent rule for entities?
- ✓ Explain how to treat residual risk

NOTES

Chapter 7

Vulnerabilities of Financial Institutions to ML and TF

Learning Objectives

- Understand the vulnerabilities of various banking functions:
    - Wealth Management
    - Lending and Credit facilities
    - Correspondent Banking
    - Investment Banking
    - International Trade Finance
- Understand the vulnerabilities of other financial sectors:
    - Insurance
    - The securities sector and financial instruments
    - Digital or virtual currencies
    - Money Transfer Businesses

Introduction

The financial services sector is a very large industry split across a wide range of services, from the classic deposit and lending banking services to the more modern electronic payments and digital currencies. Each financial services sector has different types of money laundering and terrorist financing risks. For example, in the retail banking sector we have high-volume low-value transactions requiring automated systems for effective monitoring and a fairly disconnected client-bank relation that hinders monitoring and investigation of suspicious transactions whereas in the wealth management we have low-volume but high-value transactions requiring more enhanced scrutiny.

In this Chapter we will go over some key financial industries within the banking sector and outside the banking sector. We will also see how criminals can use the services of financial institutions for their illegal purposes such as wealth management, correspondent banking, lending and credit facilities, international trade.

We will next cover the insurance sector and the use of insurance policies to launder money. Then, we will move to the securities world where we will talk about investment firms and brokers, as well as foreign exchange the growing area of digital or virtual currencies.

Finally, we are going to examine the money transfer providers and foreign exchange bureaus, which share quite a few similarities.

1. Vulnerabilities of banking services to money laundering and terrorist financing

1.1 Wealth Management

Wealth Management, otherwise known as Private Banking, is usually a division of a financial institution offering services to high-net worth clients and is mostly characterized by the low volume but high-value transactions. Due to the types of services offered and the type of clients it serves, the industry is exposed to specific money laundering risks.

Private banking activities are generally defined as "providing personalized services to high-net-worth clients". Due to the nature of this relation between the Bank and the client, there are certain vulnerabilities with regards to AML. Private bankers tend to act as client advocates, at risk of being less objective with respect to AML and compliance with laws and regulations. Powerful clients including PEPs tend to engage in private banking relations, thus exposing the Bank to a higher risk.

A wealth management department is adhering to a culture of high confidentiality with the use of secrecy jurisdictions or shell companies. The Bank has a significant profit potential from such services which might hinder the effectiveness of the internal controls in the Bank. The low-volume but high-value transactions are easier to monitor but could be problematic due to the clientele, stricter secrecy and conflict of interest.

Financial institutions offering wealth management services are particularly exposed to reputational risk and should therefore apply enhanced due diligence to such operations. Wealth management services are offered to individuals, commercial businesses, trusts, intermediaries or private investment companies. In each case, reputational risk may arise if the firm does not diligently follow established KYC procedures.

Case Study

This is a classic example of a PEP being involved in money laundering with the assistance of a private bank. Augusto Pinochet (1915-2006) was a general, politician and dictator who ruled Chile from 1973 to 1990.

A US-based bank has set up for Augusto Pinochet shell companies at overseas locations as well as a trust. Exploiting the weak AML regulations of the overseas jurisdiction at the time the bank has set these shell corporations as owners of the accounts it held. The bank has opened these multiple accounts and accepted millions of dollars in deposits from Mr. Pinochet with no serious inquiry into questions regarding the source of his wealth. Thereby, the bank was deliberately concealing the name of Pinochet from the accounts.

Furthermore, when Spanish authorities issued a freezing order for Pinochet's assets, the bank went on to completely conceal the name of Pinochet from any documents. In this case, the bank's employees knowingly colluded with him to launder the money.

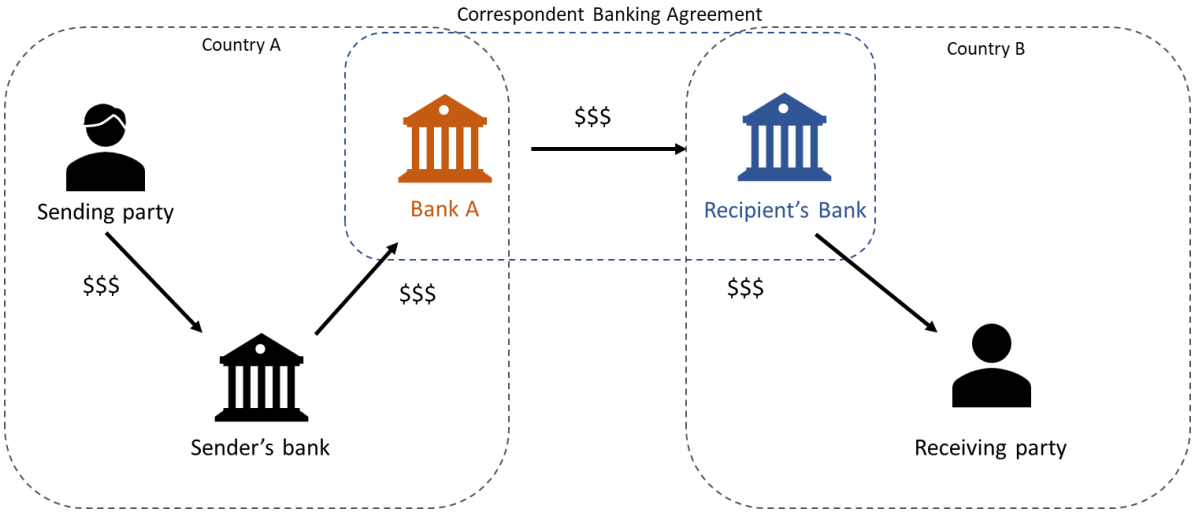
CDD procedures and monitoring

All new clients and new accounts in this department should be approved by at least one person, of appropriate seniority, other than the wealth management relationship manager. It is appropriate to have particular safeguards in place internally to protect confidentiality of wealth management customers and their business, however firms must still ensure that at least equivalent scrutiny and monitoring of these customers and their business is conducted, e.g., they must be open to review by compliance officers and auditors.

In wealth management, an effective automated monitoring system becomes a necessity due to the large volume of transactions, but it is not easy to screen flagged transactions. In such cases, as there is usually not a close relation between the customer and a named relationship manager, identifying suspicious transactions from the pool of flagged transactions becomes a challenge.

1.2 Correspondent banking

Not all banks have an international network or even a national network for smaller institutions, correspondent banking enables one, usually smaller bank (respondent bank) to use the network of another larger bank (correspondent bank) for the provision of services to its clients. This type of relationship allows smaller in size banks to undertake international financial transactions in jurisdictions where they do not have physical presence.



What is of particular interest to AML is that correspondent banks carry out financial transactions on behalf of customers of another bank. Often, there is no direct relationship between the correspondent bank and the underlying parties to a transaction. As a result, the correspondent bank is not in a position to verify the customers' identities. Furthermore, the correspondent banks often have a limited amount of information regarding the purpose of the underlying transactions, especially in the cases of electronic payments or clearing cheques. Due to the large volume of amounts following through the correspondent accounts, identifying suspicious transactions can be challenging for the correspondent bank which usually does not have the all the relevant information with regards to the transactions.

Correspondent banks are also exposed to other money laundering risks due to the non-face-to-face relation with the other bank, which is possibly in another country, in some cases with no regulations or internal controls in place. This non-face-to face business relation may be regarded as higher risk, which in return requires the use of enhanced due diligence measures. In performing this due diligence, several factors should be considered, such as: the counterparty's geographic risk, overall corporate structure, ownership and management, types of products and services offered, its customer base, prior history with regulators and its AML program. Adhering to a similar, if not a stricter, regulatory framework can certainly help to reduce the risk.

Banks are not allowed to enter into correspondent relationships with shell banks[7] or conduct any transactions with them.

1.3 Lending and Credit Facilities

Lending and credit facilities are the main revenue driving services offered by banks. These too, however, can be used for money laundering by criminals or to fund terrorist activities using a variety of methods.

One method that lending might be abused by criminals is one party to obtain a loan which is repaid by a third party (with illegal funds), but the Bank is not aware of the link between them. The purpose of obtaining the loan might just as well be used to conceal a money laundering scheme. Another method utilizes the collateral used as security for the loan or credit facility. The collateral could be a tangible asset or illegal funds deposited in another country that might just as well be a high-risk country.

Since these services rely on documentation it is also possible that false documents may be presented. Moreover, an attempt would be made to hide the trail between the illegal proceeds and the borrower. Essentially any attempt to conceal parts of a transaction should be a red flag for money laundering, thus requiring further investigation.

When providing lending or credit facilities, banks need to conduct customer due diligence in all related parties taking into consideration the relevant risk factors associated with the establishment of the business relationship.

1.4 Investment Banking

Investment Banks could be used in the layering and integration stages of money laundering, as they usually do not take deposits, since funds are transferred from deposits with a commercial bank. Nowadays Investment Banks are functioning in an international context with clients from around the world. They are therefore faced with the higher AML risk of non-face-to-face customer relations or even from higher risk countries.

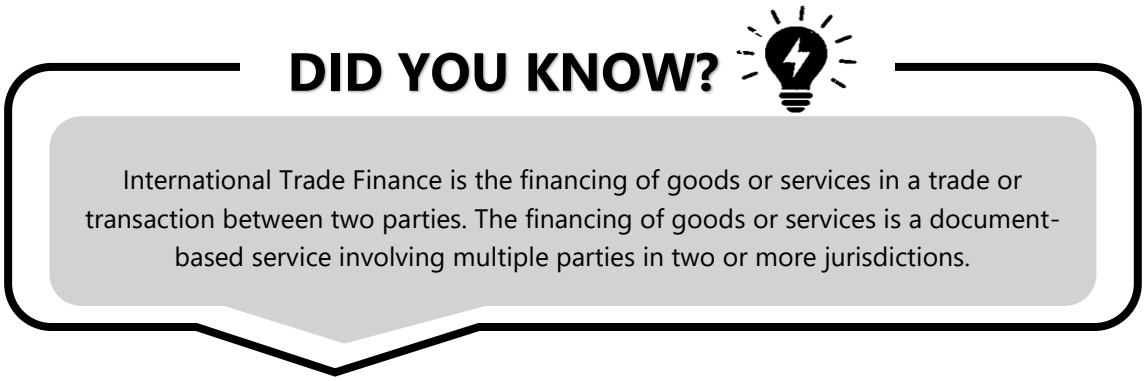
[7] According to FATF, Shell bank means a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

Investment-banking shares similar characteristics to private banking, such as a smaller number of clients but of a higher net worth. If a criminal is successful, he or she can move large sums over a large network through stock dealings, corporate financing, and other financial instruments.

Furthermore, they are often dealing with complex mergers and acquisitions and corporate financing which are the perfect kind of transactions for layering. Dealings with stocks or other financial instruments could also be used to both layer and integrate illegal proceeds, by obtaining at the end highly liquid marketable securities. Especially attractive to money launderers are low value shares, also known as penny stocks, where the regulations are laxer and are traded over-the counter or in more loosely regulated stock exchanges.

1.5 International Trade Finance

Although international trade finance is an important banking business, it brings with it some inherent AML risks and vulnerabilities.


DID YOU KNOW?
International Trade Finance is the financing of goods or services in a trade or transaction between two parties. The financing of goods or services is a document-based service involving multiple parties in two or more jurisdictions.

A key AML issue here is documentary fraud where commercial invoices or export/import documentations are falsified. Such fraud can lead to multiple outcomes in the same transaction such as circumventing sanctions, transportation of contraband or weapons to another country and launder illegal funds. Banks should not only be alert to any transactions that involve high-risk goods such as weapons, but also be aware if any goods may be excessively over or under valued thus facilitating money laundering across borders.

An example can be as follows: an importer could pay an excessive amount using illegal funds for some goods that may have a very small value or are in fact worthless. Usually this would also require the fraudulent falsification of the invoice. Other similar schemes would be double invoicing, sending only part of the goods or by using fictitious goods. If the trade is successful, then the illegal funds will appear to come from a legal commercial source. As aforementioned, since multiple parties are involved, collusion between them is necessary. The use of shell companies in such transactions is also a common practice to conceal ownership of either the goods or illegal funds.

The Bank should therefore have knowledge of the sources of funds whether from repayments or collateral. Trade financing can be abused by criminals that have international operations of

trafficking, drugs, contraband, or weaponry. In such cases many parties are usually involved, as it requires a significant paper trail in order to achieve their goals.

2. Other sectors

2.1 Insurance Products

It might be thought as odd to launder money through an insurance company, but it is in fact very much a possibility. One can purchase an investment-linked life insurance policy that is subsequently cancelled early on and the policyholder simply pays an early surrender penalty. In such a case, the client is more concerned with the termination features of the product than its performance.

Other general insurance policies are also used through false or inflated claims, which, if paid could easily cover any losses and thus legalize the original funds. Products such as bearer insurance policies are also a very attractive option for money launderers as they can easily use another person to buy the product and then give the title deed to the perpetrators just like bearer shares.

Policy loans could also be used whereby a client purchases a single premium policy and then takes out a loan. Then the client may not repay the loan and any outstanding loan amount is deducted from any future claim. Excessive payments of insurance premiums could be made and if such a case occurs, the insurance company should reimburse the excess amount at the original source or directly into a client's bank account.

2.2 The Securities Sector

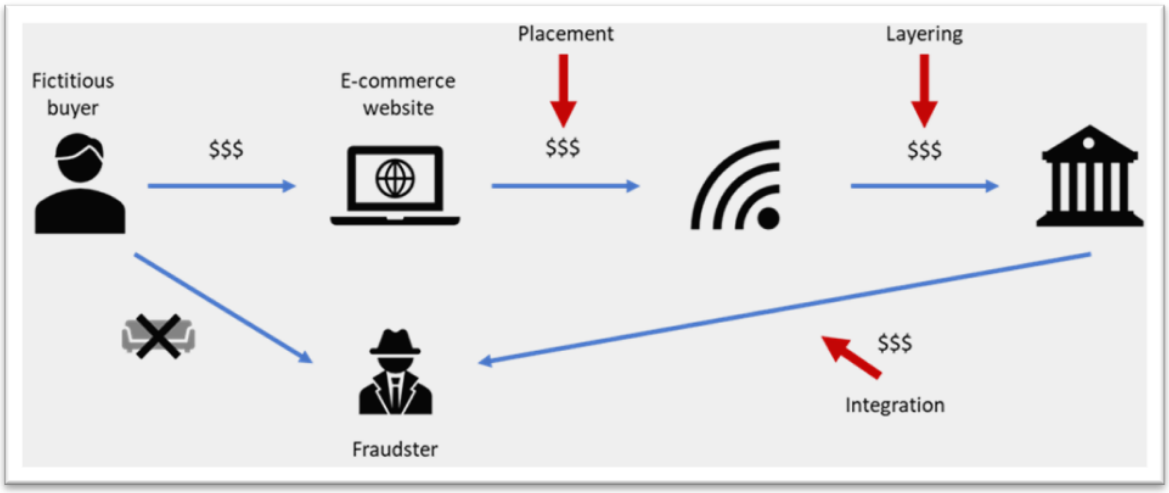
Securities involve any transferable securities, including equities and bonds or similar debt instruments, money market instruments, investment funds, options, futures, swaps, derivative instruments, and any other securities that can be traded. The securities sector is characterized by its internationality high-level of interaction, high-volume of transactions, speed, anonymity, and complexity.

Money laundering and terrorist financing risks mainly stem from the types of securities products and services, customers, investors, and payment methods used in the securities sector.

Vulnerabilities

- The global reach of the securities sector and the speed of transactions across a multitude offshore jurisdictions and financial markets is also another factor that constitutes this sector attractive to criminals who want to launder their illicitly gained funds.

- A vulnerability associated with broker-dealers is their reliance on another financial institution's KYC and CDD procedures. It could then be assumed by the broker that since the financial institution has opened an account for the client then there is no need to repeat the process. As a result, if the criminal successfully places money with the financial institution, then he or she can more easily execute transactions as part of the layering and the final integration stage. This is an AML risk for the broker but can be mitigated by doing their own KYC and CDD without relying on third parties.
- Any financial instruments that can be easily transferrable either due to their characteristics, such as bearer shares, or through a service, such as easy electronic transfer of ownership, are vulnerable to money laundering. The investment firm or broker must therefore have in place appropriate controls and safeguards to avoid this abuse. For example, a custodian instead of the client can hold bearer shares, and electronic share transfers over the Internet should have strong digital security to avoid any hacks.
- Criminals may use private companies that are in the process of going public by investing while the companies are still private and hence have less transparency. Then criminals liquidate their shares in the public stock market.
- Foreign currency trading firms, or FX trading, as they are more commonly known, are usually licensed investment firms. This is a new trend in electronic trading of financial instruments. Their products are characterized by a large number of small investors dealing with a very large number of low value transactions. Since it is electronic, almost all customers are non-face-to-face. Furthermore, as foreign exchange markets are quite volatile, it is quite normal for a customer to urge the firm to open his or her account as soon as possible to exploit a particular market move.
- It is very easy nowadays for criminals to setup a fictitious commercial website in no time. Such websites can be used by criminals to setup fictitious commercial transactions in order to launder illegal proceeds. For example, the two parties of the transaction know each other and when the purchase is executed, no physical goods are actually transferred. Due to this collusion, there are no complaints reported for a failure to deliver any goods. The website is connected to the financial system through an internet payment service provider which is in turn connected to a commercial Bank, essentially executing all three stages of money laundering all in one go.



2.3 Digital or Virtual Currencies

Virtual currencies are a new trend but now have developed into a powerful payment method with global acceptance. A virtual currency is held with a dedicated blockchain network that is decentralized, meaning that it is not controlled by a centralized banking authority, but from private users, developers, or the founders of the blockchain.

DID YOU KNOW?

Virtual currency is a digital representation of value and is only available in electronic form. It is stored and transacted only on the internet, through designated software or through digital wallets.

It is an innovative, cheap, and flexible method of payment. However, this new and unfamiliar business model poses a challenge to regulators around the world who are not sure how to deal with this payment method. While some countries have embraced this new technology, others are eliminating its legitimate use.

Transferring funds using virtual currencies has many vulnerabilities and is often very susceptible to money laundering. The reason for that is that decentralized systems are almost always completely anonymous by design. Therefore, there is a very high risk of those funds being illegal proceeds.

Virtual currencies, according to FATF, present potential money laundering and terrorist financing risks due to the following characteristics:

- the anonymity provided by the trade in virtual currencies on the internet
- the limited identification and verification of participants

- the lack of clarity regarding the responsibility for AML/CFT compliance, supervision and enforcement for these transactions that are segmented across several countries
- the lack of a central oversight body

FATF has issued a document "Key definitions and potential AML/CFT risks of Virtual currencies" and also "guidance for a risk-based approach to Virtual Currencies" recognizing that these currencies have emerged and attracted investment in payment infrastructure built on their software protocols.

The 5th AML directive also brings virtual currency exchange platforms and custodial e-wallet providers under the scope of Anti money laundering regulations and requires that these platforms need to conduct CDD and be able to associate the virtual currencies with their owners.

2.4 Money transfer and foreign exchange bureaus

Money transfer businesses and foreign exchange bureaus are sectors that have been gaining growth due to increased travel and cross-migration between countries. Money transfer providers offer their services for example to immigrants in order to send money home, and also to individuals who do not have a bank account.

A usual money laundering method in business is smurfing. In many cases, "smurfs" are used to make several structured cash transactions in smaller amounts to avoid mandatory thresholds or KYC/CDD requirements. The person used as "smurf" can execute the transactions at the same day or over a period of days through a single person acting as an agent or through several agents. The agents are also called money-mules as they get the money from criminals, execute the transfer, and get paid a commission on the amount of the transfer. Paper trail in money transfer providers is often lacking due to the low value of occasional transactions. So, transaction monitoring or investigations of this type of transactions are often very difficult tasks.

The clientele of money transfer providers demand to send money to countries that are outside of the regular international banking network, such as FATF's high risk countries. Therefore, coupled with structuring, this could be an easy way for money launderers to funnel funds through to these countries. For a foreign exchange bureau, the vulnerabilities are almost the same but instead of transferring funds, the customer is exchanging local currency to foreign currency and vice versa to effectively achieve the same result.

There are unlimited ways that criminals aim to launder their funds. Despite the strict regulations, a lot of money is laundered every year. Financial and non-financial institutions are required by national regulations and global anti-money laundering standards to put in place anti-money laundering policies and procedures to prevent from being used for these illicit purposes.

3. Learning summary

- Retail banking has AML risks due to high volume of transactions and a fairly disconnected client-bank relation for effective monitoring. Private banking has AML risks due to clientele, stricter secrecy, and conflict of interest.
- Correspondent banking has AML risks due to the non-face-to-face relation with the other bank which is possibly in another country, with no regulations or internal controls in place.
- For loan and credit facilities, illegal funds or assets may be used as collateral or to make repayments.
- Investment banking is similar to private banking but is used for layering and integration through stock dealings, corporate financing and other financial instruments.
- International trade financing can be abused along with trafficking, drugs, contraband or weaponry traded between countries. Collusion and documentary fraud are necessary to achieve laundering.
- Investment-linked insurance policies may be exploited by early surrender and general insurance policies by a claim fraud. Also, a policy loan may be taken and never repaid.
- Investment firms and brokers are vulnerable to Money Laundering because they are over-reliant on KYC/CDD procedures provided by their counterparties. Also, their vulnerability stems from dealing with bearer shares, and share trading platforms that may be hacked.
- FX trading companies deal with a large number of, usually non-face-to-face, small investors who execute a high volume of low-value transactions.
- Internet payments can be easily used by Money Launderers to setup fictitious commercial websites and perform virtual transactions. Digital currencies transactions are almost always anonymous.
- Money transfer providers and foreign exchange bureaus can be exploited through low value transactions performed frequently over a short period of time by one or more people, usually called money-mules

4. End of Chapter Questions

Think of an answer for each question and refer to the chapter content for confirmation.

- ✓ What are the vulnerabilities of:
    - Wealth management (also known as private banking)?
    - Correspondent banking relationships?
    - Lending and credit banking facilities?
    - Investment Banking?
    - International Trade Finance?
    - Insurance products?
    - The securities sector?
    - Virtual currencies?
    - Money transfer and foreign exchange bureaus?

NOTES

Chapter 8

Money Laundering and Terrorist Financing Case Studies

Introduction

Banks play an important role in helping regulators fight financial crimes, including money laundering and terrorist financing. However, regulators in many cases identify failures in the banks' anti-money laundering systems and controls and do not hesitate to impose heavy penalties. This leads to several negative consequences, including heavy penalties.

Two cases have been selected that allow for a practical perspective on how financial institutions may fail to implement adequate AML/CFT mechanisms and the impact such failures may have. The two cases are the following:

1) The **Danske Bank** money laundering scandal arose in 2017-2018. Reports have commented that around €200 billion of suspicious transactions flowed from Estonian, Russian, Latvian, and other sources through the Estonia-based bank branch of Denmark-based Danske Bank from 2007 to 2015. It has been described as possibly the largest money laundering scandal ever in Europe and as possibly the largest in world history. It includes incoming funds from Estonia (23%), Russia (23%), Latvia (12%), Cyprus (9%), UK (4%) and others (30%, more than 150 countries each of which account for a smaller part than the UK). Outgoing funds were distributed between Estonia (15%), Latvia (14%), China (7%), Switzerland (6%), Turkey (6%) and others (52%). Noted that the €200bn figure represents the suspicious transactions involved, which is a combination of legal and illicit transactions.
2) The second money laundering scandal to be discussed concerns the recent fine of 4 billion Swedish Krona ($360 million) imposed to **Swedbank AB** by the Swedish Financial Supervisory Authority with criminal investigations taking place by the Estonian authorities. **Swedbank AS** has also been ordered to improve its AML risk control systems to comply with applicable requirements. Swedbank is still under investigation by the Latvian Police Department, European Central Bank, Swedish Economic Crime Authority, and several United States authorities. It is likely that Swedbank will face additional sanctions from these authorities and that private investor securities litigation will follow.

1. Danske Bank AML Case study

Danske Bank, headquartered in Copenhagen, is the largest bank in Denmark. The bank's local branch in Estonia, which was acquired by Danske Bank as part of a merger with Finnish Sampo Bank in 2007, which was mainly involved in non-resident portfolio management. The local branch was under the jurisdiction of both the Financial Supervisory Authority of Denmark (due to the location of the headquarters) and the Financial Supervisory Authority of Estonia (due to the location of the branch), and both have blamed the other side for the deficiencies identified.

In December 2013, a whistleblower informed the Danske Bank in Denmark (Group Headquarters) of his concerns about possible ML taking place and included a report of a UK company transferring up to $20 million per day through the Estonian branch. The company held the same address in London as 64 other companies with accounts at the Estonian branch and was owned by individuals from ML havens. Following additional reports by the whistleblower, an AML review was conducted by the Group's Internal Audit and the following issues were revealed:

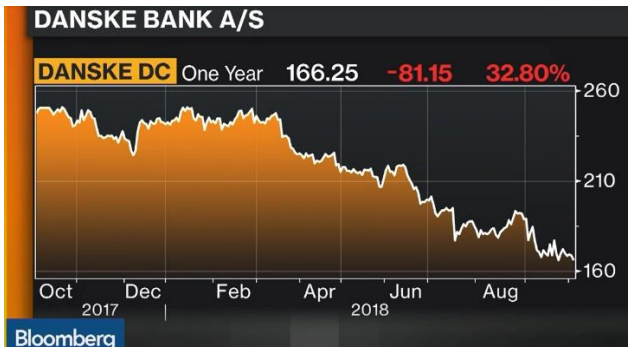
- some customers used newly formed companies in order to avoid filing financial statements
- complicated corporate structures were employed using entities in the former Soviet Union and tax havens
- the beneficial owners of corporate customers were not identified
- such information was not requested as it may have caused problems in the event that Russian authorities requested information and
- nine unregulated Russian intermediaries were used to make payments out of Russia.

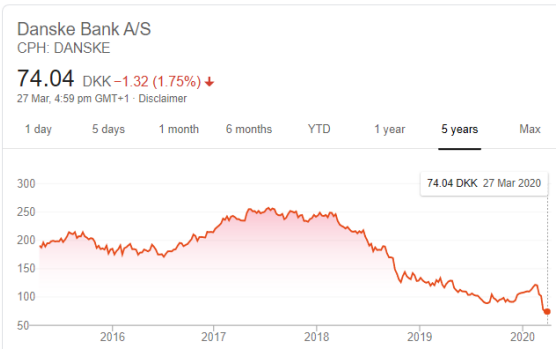
In the course of 2015 and until January 2016, Danske Bank closed the International Banking department of the Estonian branch, which was the department where the violations of the money laundering regulations primarily took place. The closing down occurred following orders issued by the EFSA in 2015, after the EFSA's two money laundering inspections in 2014.

Danske Bank has admitted that a large part of 200 billion euros in transactions at an Estonian unit were suspicious. The Copenhagen-based lender is currently cooperating with thorough investigations by the U.S. Department of Justice and the U.S. Securities and Exchange Commission, amongst others.

Effect on share price

In March 2018, when allegations that the Bank's Estonia branch was involved in money laundering between 2007 and 2015 intensified, the share price has fallen drastically.





In September 2018, Danske Bank admitted that its procedures for oversight at the Estonian Branch have completely failed and that its money laundering controls in Estonia had been insufficient. As a result, the CEO and the Chairman of the Board of Directors stepped down. In

addition, a number of employees both at the Estonian branch and at the Group level were found not to be compliant with their legal obligations and were therefore dismissed.

In February 2019, the Estonian Financial Supervisory Authority (EFSA) intimated Danske Bank to cease its activities in Estonia. At the same time, Danske Bank decided to cease its activities in Latvia, Lithuania, and Russia, in line with its strategy of focusing on its Nordic core market.

Danske Bank is currently under investigation from a range of authorities and it is expected that Danish, Estonian, European and US regulators will impose penalties. Moreover, twelve former employees in Estonia are under investigation by the Estonian State Prosecutor. It is estimated that Danske Bank will be fined $2 billion for the anti-money laundering failures.

Other European banks (Deutsche Bank, Swedbank – to be discussed below, Raffeisen Bank) are being drawn into the case for allegedly helping transfer illicit funds from Danske Bank. It is unclear at this time how long the Danske Bank money laundering case will last or how many entities it will draw in.

Correspondent banking: Deutsche Bank

The U.S. Department of Justice ("DoJ") are enquiring the bank's role in transferring suspicious funds from Danske Bank to the United States.

Deutsche Bank has until today been penalized in the United States for the anti-money laundering failures in its correspondent relationship with Danske Bank. Deutsche Bank was also imposed an additional $15.8 million from the German prosecutors for failing to submit more than 600 reports that would have alerted criminal investigators to suspicious bank transactions with regards to its controversial relationship with Danske Bank.

Other consequences

The International Securities Associations and Foundations Management Company for Damaged Danske Investors, or ISAF-Danske, represents private and institutional investors, including pension funds, insurance companies and investment managers in the US, Canada, Japan, Sweden, Luxembourg, Norway, Austria, Germany, France, Portugal, Spain and Australia.

This group of international investors managing trillions of dollars in assets has filed a series of lawsuits against Danske Bank in connection with the money laundering for €197m. The lawsuit details how Danske Bank "violated Danish capital market laws by deliberately misleading and keeping investors in the dark for years, by not disclosing that its financial income statements and retained earnings included significant earnings from known illegal high-risk money laundering activities".

In the period from 2007 through 2015, customers in the Non-Resident Portfolio generated an increasing part of profits in Danske Bank's Estonian branch:

Share in per cent	2007	2008	2009	2010	2011	2012	2013	2014	2015
Profits before credit losses	49 %	52 %	50 %	50 %	69 %	94 %	99 %	95 %	47 %
Profits before tax	51 %	79 %	n/a	67 %	42 %	51 %	76 %	71 %	40 %

Danske Bank Investigation results

According to a report prepared by legal firm Bruun & Hjejle (2018 – Link) that investigated the events and comprised a thorough examination of customers and transactions covering the period 2007-2015, there were several reasons why the case developed as it did. These include:

- a series of major deficiencies in the Bank´s governance and control systems made it possible to use Danske Bank's branch in Estonia for suspicious transactions
- since the acquisition of Sampo Bank in 2007 until 2015, when the non-resident customer portfolio was terminated, there was a large number of non-resident customers in Estonia that the Bank should have never accepted as customers and that they carried out large volumes of transactions that should have never happened
- In 2007, when acquiring Sampo Bank, the Danske Bank at group level received specific information from the Russian Central Bank through the Danish FSA pointed to possible criminal activity and money laundering not caught by Sampo Bank AML procedures. Danske Bank missed this opportunity.
- In 2013, a correspondent bank clearing USD transactions, ended up its correspondent banking relationship with Danske Bank for AML suspicions but still, the bank did not scrutinize its non-resident portfolio.
- AML procedures at the Estonian branch involving the Non-Resident Portfolio had been manifestly insufficient and inadequate.
- From 2007 through 2017, a number of former and current employees, both at the Estonian branch and at Group level, did not comply with legal obligations forming part of their employment with the bank.
- in general, the Estonian branch had insufficient focus on the risk of money laundering, and branch management was more concerned with procedures than with identifying actual risk
- The Estonian branch had its own IT platform. The branch did not have y the same customer systems and transaction and risk monitoring as the rest of the Group, and the Group did not have the same insight into the branch as other parts of the Group.
- Only a few suspicious transactions were reported to the Estonian Financial Intelligence Unit (FIU).
- as a result, the Group was slow to identify the problems and rectify the shortcomings. Although a number of initiatives were taken at the time, it is now clear that it was too little and too late.

Importantly in the report's key takeaways there is particular reference to the '*Failed AML procedures at the Estonian branch*'. Specifically points 8 and 9 note the following:

Point 8: Historical misconception of AML procedures

The Estonian branch had its own IT platform. This meant that the Branch was not covered by the same customer systems and transaction and risk monitoring as Group, and it also meant that Group did not have the same insight into the branch as other parts of Group. Many documents at the Estonian branch, including information about customers, were written in Estonian or Russian. For a long time, it was believed within Group that the high risk represented by non-resident customers in the Estonian branch was mitigated by appropriate AML procedures.

Point 9: Failed AML procedures realized by Group in 2014

In early 2014, following a whistleblower and new reporting from Group Internal Audit, Danske Bank Group realized that there had been a historical misconception. It was now realized at Group level that AML procedures at the Estonian branch involving the Non-Resident Portfolio had been manifestly insufficient and inadequate.
It was also realized that all control functions (or lines of defence) had failed, both within the branch and at Group level. This included business functions as well as Group Compliance & AML and Group Internal Audit. As demonstrated by Group Internal Audit in the first quarter of 2014 and by an external consultancy report from April 2014, (i) there had been insufficient knowledge of customers, their beneficial owners and controlling interests, and of sources of funds; (ii) screening of customers and payments had mainly been done manually and had been insufficient; and (iii) there had been lack of response to suspicious customers and transactions.

Actions taken by the Bank as remedy of the AML violations

- Closing down banking operations in Estonia and other neighbouring states.
- Developing a strong compliance culture and development of competencies.
- Strengthening the organisation's governance and updated procedures. In particular, the bank has established a new business unit, Group Development, whose purpose is to strengthen the development activities across the Group, including Group strategy, product development, partnerships and marketing.

Lessons Learned

- The world of finance today is so complicated that even with established AML/compliance programs in place, it is possible for criminals to exploit the banking or financial platforms of long-standing institutions who may not be paying close attention.
- The importance of having clear and secure procedures whereby whistleblowers are given the chance to report wrong doings to the relevant units is unequivocal. We only know about the Danske Bank scandal because of the actions of a whistleblower.
- The importance of having constant checks on systems, rather than launching a strategy and assuming it is working well was highlighted. If constant checks had been made on its three lines of defence model, the Bank could have spotted earlier on that something had broken down and addressed it accordingly.
- While foreign branches may represent only a very small part of a Group's total

operations, they may bring considerable regulatory problems if internal reporting mechanisms and any local control functions are not properly integrated into the Group structures.

- A critical question needs to be considered by a multinational corporation: to what extent branch reporting mechanisms are assessed and to what degree do they correspond with the head office?

Conclusion

- Danske Bank A/S is currently facing billion of euros of fines by authorities in Denmark, the U.S. and the U.K. following investigations into Europe's biggest money laundering scandal. The bank is also facing lawsuits from various investors.
- The Bank's share price has dropped significantly after the publication of the scandal.
- Major European banks like Deutsche Bank, Swedbank and Raffeisen Bank are connected to this AML scandal accused of helping transfer illicit funds from Danske Bank.
- The findings of the Investigation Report of the Non-Resident Portfolio Branch revealed that there was lack of knowledge of customers, lack of identification of the source and origin of funds used in the transactions, no screening of customers against PEPs as well as of incoming payments against sanctions.
- The bank proceeded with rectification actions regarding the AML violations such as closing down the banking operations in Estonia, establishing a strong compliance culture and development of competencies, investing into more employees and new IT systems and strengthening organisation and updated procedures to prevent AML violations in the future.

2. Swedbank case study

Swedbank AB (publ) ("Swedbank," or "the Bank"), a Stockholm-headquartered bank that is publicly traded on NASDAQ Stockholm (SWED), operates in four home markets: Sweden and the three Baltic markets of Estonia, Latvia, and Lithuania. The Bank has three primary business lines: Large Corporates and Institutions ("LC&I"), which handles large corporations and financial institutions; Swedish Banking, which handles private customers and companies in Sweden; and Baltic Banking, which covers Swedbank's business in the three Baltic states. Baltic Banking operates through three main subsidiaries: Swedbank AS (Estonia) ("Swedbank Estonia"), Swedbank AS (Latvia) ("Swedbank Latvia"), and Swedbank AB (Lithuania) ("Swedbank Lithuania") (collectively, the "Baltic Subsidiaries"). Swedbank also maintains several international branches, including one in New York USA. One of the oldest financial institutions in Sweden, Swedbank through its predecessor entities has been in existence for 200 years.

In late 2018, media reports raised questions regarding Swedbank's exposure to money laundering scandals involving the Baltic region and Estonia in particular. At the time, Swedbank publicly maintained that it had limited exposure to such risks because Swedbank was a low-risk bank focused primarily on domestic retail customers, and because Swedbank had anti-money laundering ("AML") procedures in place to ensure that it acted forcefully in response to suspicious activity.

On 20 February 2019, the Swedish public television network program Uppdrag granskning, broadcast on Sveriges Television ("SVT") began a series of broadcasts alleging that customers of Swedbank's Baltic Subsidiaries had engaged in suspicious transactions indicative of money laundering. Subsequently, the Swedish Financial Supervisory Authority ("SFSA") and Estonian Financial Supervisory Authority ("EFSA") announced investigations into the allegations.

On 19 March 2020 the Swedish Financial Supervisory Authority (FSA) announced (Link) that following serious deficiencies in the management of the risk of money laundering in its Baltic operations, it decided to issue Swedbank AB a warning and an administrative fine of 4 billion SEK (approximately €360 million). This was the first sizable penalty Swedbank received after the laundering scandal erupted in the previous year. The investigation of the Estonian FSA reached similar conclusions noting that the Estonian subsidiary had severe deficiencies in its anti-money laundering risk control systems and that the bank failed to live up to the anti-money laundering requirements.

The issue of whether money laundering or other criminal acts took place in the bank are currently being investigated by the Estonian Prosecutor's Office. As in many other countries, double jeopardy is not permitted in Estonia, and therefore Estonian FSA terminated its own misdemeanour investigation into Swedbank AS in November 2019 to allow the prosecutor to continue with its criminal investigation.

Following the fine imposed on **Swedbank AB** (the "Bank"), Clifford and Chance (a legal firm) published a report requested by the Bank, where the legal firm was instructed to carry out a probe into the Bank's Baltic operations. The Bank has published the report of the investigation

(the "Report"), issued on March 23, 2020, and is available on its website. The investigation sought to identify historical deficiencies in Swedbank's AML compliance systems and controls from January 2007 through March 2019 and focused on the areas of Swedbank and the Baltic Subsidiaries that evidenced the highest historical AML-related risks.

The Report revealed that between 2014 to 2019, Swedbank's branches in the Baltic region (including Estonia, Latvia, and Lithuania), processed roughly €17.8 billion ($19.4 billion) in payment into customer accounts and €18.9 billion ($20.7 billion) in payments from customer accounts. The Report found that these transactions alerted on three or more of 21 algorithmic detection scenarios utilized in the investigation to identify potentially suspicious transactions.

The Report revealed that from before 2007 through 2016, Swedbank Estonia and Swedbank Latvia actively pursued certain high-risk customers as a business strategy. For example, Swedbank Estonia accepted certain customers that had been off boarded by another Estonian Bank in 2015 that had decided to exit the high-risk non-resident ("HRNR") business due to money laundering risks.

The Report also found that although the Estonian branch formed a special committee to review the on-boarding and regulation of HRNR customers, the committee still approved high risk customers without having complete documentation regarding the ultimate beneficial owners, proof of source of funds or explanation of the legitimate business purpose of the customers and did not address red flags.

In addition, some Estonia branch employees kept certain information regarding the ultimate beneficial owners for some customers outside of the bank's regular customer database. Employees of Baltic branches overlooked or disregarded indications of potentially suspicious transactions. Certain high-risk customers of Baltic branches were allowed to open accounts in other Swedbank regions.

Swedbank Governance

The Report found that senior management historically failed to establish clear lines of AML-related responsibilities. It noted that the three CEOs that had led Swedbank throughout the review period lacked adequate appreciation of the severe risk posed by HRNR customers in its Baltic banking.

The Report also found that the degree and seriousness of the AML control deficiencies were not appropriately escalated to the Board in a timely manner. The Report further found that Swedbank did not always take an "actively transparent posture" with regulators regarding AML-related issues.

Violations of United States Regulations

The Report further assessed potential non-compliance with United States Treasury Department's Office of Foreign Assets Control ("OFAC") by Swedbank's Baltic subsidiaries or their customers.

The Report identified potential violations of OFAC regulations within the payments processed by the Baltic subsidiaries from 2014 through 2019 including 586 outgoing and incoming

transactions totalling approximately $4.8 million involving persons in Iran, Cuba, or Crimea. The Report notes that none of the suspect transactions involved OFAC-listed persons.

Actions taken by Swedbank

In order to ensure the effective establishment and implementation of a company culture opposing money-laundering and terrorism financing, Swedbank has, among others, the following procedures in place:

- Swedbank has adopted a Policy on prevention of money-laundering and counter-terrorist financing that requires all parts of the Swedbank Group to develop and implement effective programs to comply with applicable laws.
- Customer due diligence (CDD) includes, among other things, identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from reliable and independent sources. According to the Bank's website: "*We also need to understand the ownership and control structure of our customers*".
- The Group performs daily screening of the customer base against financial sanctions and PEP lists. All international payments are also screened in real time in regard to financial sanctions.
- The initiation or maintenance of a business relationship with a PEP or other relevant high-risk customer needs to be approved by an authorized decision-maker.

Conclusion

- Swedbank AB was fined with 4 billion Swedish Krona imposed by the Swedish FSA. Its subsidiary, Swedbank AS was also ordered to improve its AML risk control systems to comply with applicable requirements.
- Algorithmic detection scenarios detected €17.8 billion transactions were processed between 2014 to 2019 by Swedbank's branches in the Baltic region into customer accounts and €18.9 billion in payments from customer accounts.
- The Investigation Report conducted by Clifford and Chance revealed that although the Estonian branch formed a special committee to review the on-boarding and regulation of High-Risk Non-Resident customers (HRNR), the committee still approved high risk customers without having complete documentation regarding the ultimate beneficial owners, proof of source of funds or explanation of the legitimate business purpose of the customers, and did not address red flags.
- In summary, the Investigation Report of investigation regarding the Swedbank money laundering allegations revealed the following issues in AML compliance and enforcement:
  - the need to implement adequate systems to manage high-risk customers.
  - the need to identify beneficial ownership.
  - the need for top management to understand and truly respect AML compliance.
  - the need for transparency with regulators; and
  - the need for transparency by financial institutions with investors and the public.
- Swedbank has taken a series of actions to ensure compliance with AML provisions such as a Global-wide AML policy, effect customer due diligence (CDD) and daily screening of the customer base against financial sanctions and PEP lists.

NOTES

Chapter 9

Glossary of Terms

Accountability

Accountability can be defined as being held responsible or answerable for one's actions or lack thereof. This encompasses issues of blameworthiness, liability and one's responsibility to give an honest account of what has transpired in any given situation.

Antitrust

Antitrust laws are regulations that have been developed by governments to protect consumers from predatory business practices, limit the power amassed by a single or small group of companies, and ensure fair competition. These rules focus on a series of questionable business activities such as market allocation, bid rigging, price fixing, oligopolies and monopolies.

Audit Program or Plan

An audit program, also referred to as an audit plan, is a plan that documents the different audit procedures an auditor will perform or follow to validate that a firm has complied with its regulatory obligations. Developing such a plan is crucial to determine those areas of greatest risk and carry out the audit process in an effective manner.

Blacklist

In the financial world, a blacklist is a list of jurisdictions that have not been deemed cooperative when it comes to the battle against money laundering, tax evasion and avoidance, and financial terrorism. These types of lists are released to exert pressure on these countries to fall in line and put in place the necessary regulations to curtail illicit practices. Such lists are updated on an ongoing basis with countries either added or removed based on their overall performance in tackling these issues.

Bribery

Bribery is the practice of giving, receiving, offering or asking for money or any other valuable asset to influence a decision often being made by someone in a position of power or control. Generally, bribery involves governmental officials or members of a corporation. Bribery is proved in a court of law when it is shown that the bribe's recipient has actually made a change to their behaviour on behalf of the person handing out the gift.

Basel Committee

It was established in 1974 by the central Governors of the Group of 10 countries. Its headquarters are at the Bank for International Settlements in Basel and its purpose is to enhance financial stability by improving the quality of banking supervision worldwide. It also serves as a forum for regular cooperation between tis member countries on banking supervisory matters. It now has 45 members from 28 jurisdictions.

Bearer Share

A bearer share is equity security wholly owned by the person or entity that holds the physical certificate. The issuer firm does not register the owner of the share nor tracks transfers of ownership. For this reason, bearer shares have been abused by money launderers who seek anonymity. In many national regulations, the use of this type of shares is prohibited. In EU, the 4th AML directive requires obliged entities to prevent misuse of bearer shares by identifying their owners.

Beneficial Owner

A natural person who owns or controls directly or indirectly more than 25% of the shares or has an ownership interest of more than 25% in an entity, including bearer shareholders. It also includes those persons that exercise ultimate effective control over a legal entity.

Collateral

An asset accepted by the lender as a security for the repayment of a loan. If the borrower defaults on the repayment of his loan, the lender can seize the collateral and sell it to recover some of his losses.

Concentration risk

The potential for loss resulting from too much credit or loan exposure to one borrower or group of borrowers.

Confidentiality

Confidentiality is a set of rules or a promise that limits or places restrictions on the access to certain types of information.

Corporate vehicles

Legal entities such as limited or public companies, trusts, non-profit organisations, partnerships, or private investment companies. Often, various types of corporate vehicles are used by money launderers in combinations, in many cases involving various jurisdictions to create complexity and maximise anonymity.

Correspondent banking

The provision of banking services by a "correspondent bank" to a "respondent bank". A "correspondent bank" is a large international institution which acts as the correspondent of other smaller banks that cannot offer their services to other jurisdictions. Correspondent banks act as intermediaries, providing services with regards to wire transfers, check clearing services, payable-through accounts and foreign exchange services.

Currency smuggling

The movement of large quantities of cash cross-border, often to jurisdictions where there are no strong anti-money laundering controls.

Custodian

A legal person who was assigned with the responsibility to safekeep a person's asset in physical or electronic form.

Customer Due Diligence (CDD)

Involves the policies and procedures that enable an obliged entity to identify customers' transactions that may be related to money laundering. This includes the establishment of the identity of its customers, the expected behaviour and activity with the purpose to identify transaction outside of what is normal and expected from the customer. According to FATF, this includes 1. Identifying the customer, 2. Identifying the beneficial owner, 3. Understanding the purpose and intended nature of the business relationship and 4. Conducting ongoing due diligence and scrutiny of transactions.

Designated Non-Financial Businesses and Professions (DNFBPs)

According to FATF, DNFBPs means:

1. Casinos
2. Real estate agents
3. Dealers in precious metals and stones
4. Lawyers, notaries, accountants and other independent legal professionals.
5. Trust and Company Service Providers (TCSPs)

Egmont Group

It is a group of national FIUs that aim to create a forum for FIUs around the world and enhance their cooperation mainly with regards to communication, information exchange and training.

Electronic money

The quantity of monetary value stored on an electronic device used to make payments to other persons or entities.

Enhanced Due Diligence

Obtain additional information as part of the customer due diligence, including additional measures that will enable an obliged entity to identify and mitigate the risk associated with a high-risk business relationship. It provides a greater level of scrutiny to identify risks that cannot be detected by standard customer due diligence measures.

European Commission

A European executive body drafting proposals for new European legislation and implements decisions taken by the European Parliament and the Council of Europe.

European Supervisory Authorities (ESAs)

European supervisory bodies each responsible for a different financial sector. They include the European Banking Authority (EBA), the European Securities and Market Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA).

European Union (EU)

Created by the Maastricht treaty which entered into force in 1993 to enhance political and economic integration of countries that were mainly located in Europe. The European Union has a standard system of laws that apply in all member states with regards to the free movement of people, goods, services and capital within the internal market. In 2020, the United Kingdom was the first country that left the European Union. It is comprised today by 27 country members.

Financial Action Task Force (FATF)

An inter-governmental body created in 1898 by the Group of Seven industrial nations to foster the establishment of international standards to combat money laundering and terrorist financing. It assesses and monitors compliance of its members with the FATF standards, conducts typologies studies of money laundering and terrorist financing methods, trends and techniques and responds to new and emerging threats such as proliferation financing.

Financial Intelligence Unit (FIU)

A central, national agency responsible for receiving, analysing, and transmitting to the competent authorities reports of suspicions identified and filed by the private sector. It is an intermediary between private entities and the law enforcement agencies in the fight against money laundering, terrorist financing and other financial crimes.

GOPAC Anti-Money Laundering Global Task Force (AML-GTF)

The Anti-Money Laundering Global Task Force (GTF-AML) works with anti-money laundering experts, and organisations such as the Financial Action Task Force (FATF), the World Bank, the International Monetary Fund (IMF), the United Nations Office on Drugs and Crime (UNODC), Interpol, the Egmont Group, and Transparency International. The GTF-AML has developed a complementary approach to combating money laundering, in particular the laundering of corrupt money, and promotes the use of practical tools and techniques to limit or arrest such activity.

Human Trafficking

The trade of humans with the purpose of forced labour, sexual slavery, or commercial sexual exploitation.

Inherent Risk

The exposure of a firm to money laundering and other financial crimes in the absence of any measures and controls.

Integration

The final stage of the classic money laundering process where “dirty money” is integrated in the financial system giving the funds an appearance of “legitimacy”.

International Monetary Fund (IMF)

The International Monetary Fund (IMF) is an organisation of 190 countries, working to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world.

International Money Laundering Information Network (IMOLIN)

IMoLIN is an Internet-based network assisting governments, organisations and individuals in the fight against illicit financial flows, money laundering and the financing of terrorism. IMoLIN has been developed with the cooperation of the world's leading anti-money laundering organisations.

International Organisation of Securities Commissions (IOSCO)

The International Organisation of Securities Commissions (IOSCO) is the international body that brings together the world's securities regulators and is recognized as the global standard setter for the securities sector. IOSCO develops, implements and promotes adherence to internationally recognized standards for securities regulation. It works intensively with the G20 and the Financial Stability Board (FSB) on the global regulatory reform agenda.

Interpol

The International Criminal Police Organisation is an intergovernmental organisation with 194 member countries that helps police in all of them to work together to make the world a safer place. To do this, Interpol enables them to share and access data on crimes and criminals, and offers a range of technical and operational support.

Know Your Customer (KYC)

The measures and controls taken by an obliged entity to determine the true identity of the customer and the "normal and expected" activity. The purpose of KYC is to ensure that the money laundering and terrorist financing risk of the customer is assessed before onboarding.

Layering

The second stage of the classic money laundering process where the launderer is trying to disguise the link between the funds and their source by creating several complex financial transactions to provide anonymity. The purpose of the launderer is to make it difficult for the authorities to detect that the funds are illegal.

Legal risk

The potential for lawsuits, adverse judgments, unenforceable contracts, fines, and penalties generating losses, increased expenses for an organisation, or even the closure of the organisation.

Money laundering

The process of concealing or disguising the existence, source, movement, destination or illegal application of illicitly- derived property or funds to make them appear legitimate. It usually involves three basic stages: placement, layering and integration.

Money Laundering Compliance Officer (MLCO)

Also known as Money Laundering Reporting Officer (MLRO). It is the person responsible for overseeing an obliged entity's anti-money laundering program, controls and measures. It is a member of senior management.

Money Transfer Businesses (MTB)

Also known as Money Service Businesses (MSB) are authorized financial institutions that accept cash in one location and pay the corresponding amount to a beneficiary in another location through a clearing network to which the money transfer business belongs. This service is provided through the regulated financial system.

Monitoring

The measures and controls undertaken by an obliged entity to review its customers for unusual or suspicious patterns that are not consistent with the customer's economic profile.

MONEYVAL

Established in 1997, is the Committee of Experts on the Evaluation of AML measures and the financing of terrorist. It is a permanent body of the Council of Europe, entrusted with the task of assessing compliance of its members with FATF's 40 Recommendations.

Non-profit organisation

A legal entity which operates for the public or social benefit. When the revenues exceed the expenses, the funds are not taken by private parties but are used in line with the purpose of the organisation. Examples include political organisations, churches, social clubs, fund-raising committees etc. Non-profit organisations are often being misused by terrorists.

Obliged entity

A firm that is subject to anti-money laundering regulations and is effectively supervised.

Offshore company

A company based in any country other than the investor's home country. A company may legitimately move offshore for tax avoidance however offshore companies can also be used for money laundering and concealment of funds for tax evasion.

Operational risk

This is the potential for loss resulting from inadequate internal processes, personnel, or systems or from external events.

Payable-through account

An account opened in a large financial institution at the request of a foreign financial institution. The account enables the customers of the foreign institution to engage in banking activities and transactions in a way that they have direct control over the funds in the account.

It is difficult for the institution that provides the payable-through account to conduct due diligence to the customers of the foreign financial institution that are using the account.

Placement

The initial stage of a classic money laundering process which involves the physical disposal of illegally derived cash into the financial system.

Politically Exposed Person (PEP)

An individual who has been entrusted with prominent public functions in a foreign country, such as a head of state, senior politician, senior government official, judicial or military official, senior executive of
a state-owned corporation or important political party official, as well as their families and close associates. Each country is expected to define the term "PEP" in its national legislation.

Predicate offence

Any serious crime that generates proceeds and may constitute the subject of a money laundering offence. Each individual country specifies in its national legislation what constitutes a predicate offence within its territory. In EU, the 6th AML directive provides a harmonized list of predicate offences to close the loopholes in the criminalisation and prosecution of criminals between EU member states.

Private Banking

Also known as Wealth Management, is a department of a financial institution which provides tailored services to high-net worth individuals. The private banking services are characterized by confidentiality, complexity of transactions, establishment of investment vehicles.

Private Investment Company

A corporation established in an offshore jurisdiction with low tax transparency and high bank secrecy regulations with the purpose to protect the privacy of its owners.

Red flag

A warning signal that would trigger suspicions for the engagement of the customer in money laundering or terrorist financing.

Reputational Risk

The potential that adverse publicity regarding an organisation's business practices and associations, whether accurate or not, will cause a loss of public confidence in the integrity of the organisation.

Residual Risk

The risk that remains after controls are applied to the inherent risk.

Respondent Bank

A bank which opens an account and uses the services of another larger bank (the correspondent bank) with the purpose to provide services to its customers in jurisdictions where it does not have presence.

Risk-based approach (RBA)

Identifying and assessing money laundering risks taking into consideration factors such as customer risk, geographical risk, product, service and transaction risk and delivery channel risk.

Shell bank

According to FATF, it is a bank that has no physical presence in the country in which it is incorporated and licensed, and which is unaffiliated with a regulated financial group that is subject to effective consolidated supervision.

Smurfing

A common method used in money laundering which involves multiple individuals employed to execute multiple transactions such as cash deposits in amounts under the reporting thresholds.

Structuring

Is a method where a large amount of cash is divided in smaller amounts under the reporting threshold. The amounts are then deposited in one of several financial institutions. The purpose is to avoid triggering a filing by the financial institutions.

Supervisory Authorities

The designated competent authorities with the responsibility of ensuring compliance of obliged entities with the anti-money laundering and terrorist financing regulations.

Suspicious activity

An activity inconsistent with the customer's known legitimate business or personal activities or outside the economic profile of the customer.

Tax Haven

Countries that offer to foreign individual or businesses tax incentives and share little or no financial information with foreign tax authorities. Usually, they do not require residency or business presence for individual or businesses that benefit from their tax policies.

Terrorist Financing

It is the provision of support such as financing of terrorist acts, terrorists, or terrorist organisations.

Tipping-off

A criminal offence for notifying a person that he is the subject of a money laundering investigation or when an individual discloses information that could affect the investigation.

Trade Finance

Financial instruments or products used by companies to facilitate international trade. Trade finance provides the exporter with payment according to an agreement while the importer may extend credit to fulfil the trade order.

Trust

A legal arrangement where one party (the settlor or trustor), gives the right to another party (the trustee) the right to hold in custody assets for the benefit of another third party (the beneficiary or beneficiaries). They provide legal protection for the assets in custody and ensure that they are distributed according to the wishes of the settlor as stated on the trust deed. Trusts have been abused by criminals to provide anonymity.

United Nations

An international organisation established in 1945 and is made up of 193 member states. Through its United Nations Office on Drug and Crime (UNODC) it aims to make the world safer from drugs, organised crime, corruption, and terrorism.

Virtual Currencies

A medium of exchange that is stored and operated on a blockchain through the internet. It is a digital representation of value that is only available in electronic form. Virtual currencies do not exist in a physical form, neither are controlled by a central bank.

Wilful blindness

The avoidance of knowledge of the facts or ignoring obvious money laundering red flags. It is equivalent of actual knowledge of the illegal proceeds or the intention of a customer in a money laundering transaction.

Wire transfer

An electronic transfer of funds from one person or entity to another through a network administered by banks or financial institutions. It is considered a safe way for transmission of funds in different geographic locations around the globe.

Wolfsberg Group

A non-governmental association of thirteen global banks that has focused on developing financial industry standards for anti-money laundering (AML), know your customer (KYC) and counter terrorist financing (CTF) policies among other

NOTES

Chapter 10

Practice Questions

Disclaimer: The practice questions contained within this chapter are not meant to indicate the length or composition of the actual AGRC Examination questions. They are only meant to help candidates review the content of the examination manual

1. The basic stages of money laundering are layering:
    a. Structuring and integration.
    b. Placement and integration.
    c. Layering and smurfing.
    d. Integration and smurfing.

2. Select the correct statement:
    a. Terrorist financing and money laundering are both always derived from illegitimate sources
    b. Terrorist financing and money laundering are using similar methods to disguise the link of the funds with their source.
    c. Terrorist financing and money laundering involve both large amounts of money.
    d. Terrorist financers and money launderers have similar and often the same motives for committing their crimes.

3. The use of wire transfers is made at which stage of the money laundering process?
    a. Layering
    b. Placement
    c. Integration
    d. Layering and integration

4. Smurfing, in an AML context is:
    a. Using various individuals to invest abroad in small amounts under the reporting threshold.
    b. Using various individuals to assist in committing a financial crime so as to enable the criminal to remain anonymous
    c. Using various individuals to execute cash transactions under the reporting thresholds
    d. Using various individuals to commit several small crimes and they get a commission.

5. Which three of the following are money laundering offences?
    a. Concealing or disguising criminal property

b. Acquiring, possessing, or using criminal property
c. Aiding and abetting
d. Committing a terrorist attack

6. In 2012, the FATF has issued how many recommendations?
    a. 40
    b. 40+9
    c. 49
    d. 37

7. The 4th AML Directive foresees that member states should conduct risk assessments at country level by:

    a. Accepting only low risk customers
    b. Identifying the dangerous clients
    c. Identifying the major money laundering and terrorist financing risks in their territory
    d. Reviewing the money laundering and terrorist financing risks every year.

8. The members of the Egmont Group are:
    a. Financial Intelligence Units
    b. Countries
    c. Competent authorities around the world
    d. International global banks

9. With regards to predicate offences, the 6th AML Directive aims to:
    a. Provides a harmonized definition of the predicate offences within EU member states
    b. Provides guidance to regulated entities on how to identify possible predicate offences.
    c. Brings under the AML scope virtual currency exchange platforms.
    d. Focuses on the risk-based approach

10. What is the FIU of the UK?
    a. SEC
    b. FCA
    c. FSA
    d. NCA

11. How can an obliged entity ensure compliance of every employee within the organisation?
    a. Establish an independent audit function to test the employee compliance
    b. Include compliance with anti-money laundering regulations as a prerequisite for employment

c. The AML officer should personally contact every new employee and inform him about his responsibility orally
d. Provide appropriate training explaining the consequences of non-compliance

12. Who is responsible to submit a suspicious transaction to the FIU?
    a. One of the senior managers of the obliged entity
    b. The MLCO after getting approval from senior management
    c. The MLCO
    d. The employee who has detected the suspicion.

13. The clients' acceptance policy (select 2):
    a. sets out the criteria for accepting new customers
    b. sets out the criteria for the proper design of anti-money laundering measures and controls
    c. Establishes the type of customers that are not accepted by the obliged entity
    d. Identifies high-risk customers

14. An MLCO gets an internal suspicious report and he decides to report him to the FIU. However, the senior manager is willing to take 100% responsibility and asks the MLCO not to report him to the FIU providing his written approval. What steps would be more appropriate in order to avoid possible prosecution?
    a. Report the customer to the FIU
    b. Obtain the senior manager's approval and not report while keeping the account of the customer under close monitoring.
    c. Obtain the Board of Directors approval as an additional measure to the senior manager's written approval.
    d. Ignore suspicious activity but have the accounts closely monitored

15. The basic elements of a strong anti-money laundering compliance program are (select 3):
    a. To establish appropriate anti-money laundering policies, controls and procedures on a risk-based approach
    b. To designate a money laundering compliance officer for the oversight of the compliance function
    c. To design an ongoing employee training program
    d. To ensure compliance with anti-money laundering standards and regulations

16. The FATF recommendations are:
    a. Principle-based
    b. Policy-based
    c. Risk-based
    d. Legal obligation

17. According to the risk-based approach, which factors should an obliged entity take into consideration when assessing the risk associated with a business relationship (select 3)?
    a. Customer risk factors
    b. Product, service, and transaction risk factors
    c. Financial risk factors
    d. Delivery channel risk factors

18. The risk-based approach involves measure and procedures such as: (select 2):
    a. Monitor all high-risk customers and customer from countries with strategic deficiencies in their anti-money laundering regimes
    b. Identifying and assessing money laundering and terrorist financing risks
    c. Documenting the policies, measures, procedures for the prevention of money laundering and terrorist financing
    d. Identifying terrorist financing suspicious transactions within a specific territory

19. The FATF requires countries requires countries to perform a national risk assessment that:
    a. enables countries to understand how money laundering and terrorist financing risks interact within several sectors in the economy and take appropriate measures to mitigate these risks.
    b. Will allow the FATF assess each country its compliance with FATF 40 recommendations
    c. enable countries to obtain an understanding of the ML/TF risks they are exposed to and ensure that they have in place measures that are commensurate with the risks identified.
    d. identifies the level of risk for each financial and non-financial sector within the specific country.

20. When weighting risk factors, firms should ensure that (select 2):
    a. weighting should enable the senior management to over-ride any automatically generated risk scores
    b. weighting is not unduly influenced by just one factor.
    c. economic or profit considerations may influence the risk rating up to a degree.
    d. weighting does not lead to a situation where it is impossible for any business relationship to be classified as high risk.

21. What are CDD measures that an obliged entity needs to apply (select 3)?
    a. Identifying the customer and verifying the customer's identity using a reliable and independent source
    b. Identifying the beneficial owner and verifying the beneficial owner's identity

c. Identifying and managing customer's money laundering and terrorist financing risks
d. Conducting ongoing due diligence on the business relationships

22. Obliged entities are required to maintain all necessary records on transactions for:
    a. 2 years
    b. 5 years
    c. 7 years
    d. 10 years

23. When applying Simplified Due Diligence measures obliged entities may (select 3):
    a. Adjust the timing of CDD
    b. Adjust the type of verification documents required
    c. Adjust the frequency of CDD updates
    d. Adjust the quality of information

24. What is the purpose of Customer Due Diligence (CDD)?
    a. Identify your customers and collect documents to be able to demonstrate to the competent authorities the risk level of the customer
    b. Identify high-risk customers
    c. Identify and verify your customer and understand the nature of the business relationship
    d. To enable the MLCO to decide whether to apply SDD or EDD

25. A compliance officer has reported a suspicious transaction to the FIU. What are the steps he/she needs to follow?
    a. Inform senior management about the reporting.
    b. Remain the central point of contact with the FIU.
    c. Inform the customer that he has been reported and obtain clarifications required for the investigations.
    d. Inform all relevant employees and have the account closely monitored.

26. EU sanctions aim to (select 3)
    a. preserving peace
    b. protect human rights
    c. Ban sanctioned persons to travel in the EU
    d. strengthen international security

27. How can an organisation manage the residual risk (select 3)?
    a. Avoid the risk
    b. Transfer the risk
    c. Accept the risk
    d. Prevent the risk

28. Secondary Sanctions may be also referred to as:
    a. Extraterritorial sanctions
    b. Comprehensive sanctions
    c. Territorial sanctions
    d. Non-compliance sanctions

29. Select what is appropriate:
    a. EU institutions are obliged to comply with US Sanctions
    b. EU institutions are obliged to comply with OFAC Sanctions
    c. Multilateral sanctions involve two or more countries deciding together to impose a sanctions regime
    d. No sanctions can be imposed unless two or more countries decide together to impose a sanctions regime

30. Sanctions can target (select 3):
    a. Individuals committing a predicate offense
    b. entities providing the means to conduct the targeted policies
    c. groups or organisations such as terrorist groups
    d. individuals supporting the targeted policies

31. A wealth manager establishes a business relationship with a high-net worth customer who has personal links in a high-risk third country. What would be the next step he needs to follow?
    a. To get approval from a senior manager for the establishment of the business relationship with the customer.
    b. To proceed with the establishment of the business relationship and categorize the customer as high-risk.
    c. Do not proceed with the establishment of the relationship since the risk is too high.
    d. Report the customer to the relevant competent authorities.

32. Select the correct statement:
    a. The insurance sector is not vulnerable to money laundering
    b. Insurance policies where the premium is low and cannot be used as collateral is an attractive option for terrorist financers.
    c. In the insurance sector, bearer insurance policies are an attractive option for money launderers
    d. Insurance policies that invest in complex transactions are attractive to criminals.

33. Select the <u>two</u> correct statements:
    a. Virtual currencies are a digital representation of value that does not exist in physical form
    b. Virtual currencies are a digital representation of value that exists in physical form

c. Virtual currencies are not attractive to criminals because they are regulated
d. Virtual currencies are attractive to criminals due to the anonymity they offer

34. A broker is approached by a client. He wants to transfer an amount of €100.000 from an EEA institution in his name to invest in transferable securities. He is travelling a lot and it is difficult to provide evidence about the source of funds. The broker is thinking that the amount is from an EEA institution therefore there is a low money laundering risk since it is a regulated institution and has conducted CDD for the specific funds. What would be appropriate for the broker to discharge his legal obligation with regards to CDD?
    a. Insist that the customer should provide him with the appropriate evidence for the source of funds
    b. Accept the funds taking into consideration that the funds are coming from a regulated EEA institution
    c. Terminate the account and consider making a suspicious report to the FIU.
    d. Obtain senior management approval for the transaction and accept the funds.

35. As part of the customer due diligence, the correspondent banks should (select 3):
    a. Conduct enhanced due diligence on the Compliance officer of the respondent institution.
    b. Consider the geographical risk of the respondent institution
    c. Conduct enhanced due diligence to the respondent bank
    d. Ensure that the correspondent account will be sufficiently monitored by the monitoring systems of the correspondent bank.

36. Wealth management is characterized by:
    a. high-volume, low-value transactions.
    b. low-volume, high-value transactions.
    c. high-volume, high-value transactions
    d. low-volume, low-value transactions

37. Select the ***wrong*** statement:
    a. It is prohibited to accept clients subject to sanctions.
    b. It is allowed to accept clients subject to sanctions, but you should always conduct enhanced due diligence.
    c. An obliged entity, when assessing the money laundering risk of a customer needs to consider customer risks, geographical risks, product service and transaction risks and delivery channel risks.
    d. You are not allowed to rely on a third party for your CDD requirements.

38. Monitoring of customers' transactions should be made:
    a. On a weekly basis and in real-time
    b. According to the risk classification of the customer
    c. On a weekly basis
    d. According to the obliged entity's policy

39. The majority of governments around the world believe that the risk-based approach is preferable to a more prescriptive approach in the area of AML/CFT because it is more (select 3):
    a. Flexible
    b. Effective
    c. Proportionate
    d. Applicable

40. Designated Non-Financial Businesses and Professions include:
    a. Credit institutions
    b. Financial institutions
    c. Accountants and legal professionals
    d. Issuers of bearer shares

ANSWERS

1. B	2. B	3. A	4. C	5. A, B, C
6. A	7. C	8. A	9. A	10. A
11. D	12. C	13. A, C	14. A	15. A, B, C
16. A	17. A, B, C	18. B, C	19. C, D	20. B, D
21. A, B, D	22. B	23. A, B, D	24. C	25. B
26. A, B, D	27. A, B, C	28. A	29. C	30. B, C, D
31. A	32. C	33. A, D	34. A	35. B, C, D
36. B	37. A	38. A	39. A, B, C	40. C

Reference Materials

1. AML Global Organisations

Asia Pacific Group on Money Laundering (APGML)
The Asia/Pacific Group on Money Laundering is an inter-governmental organisation, consisting of 41 member jurisdictions, focused on ensuring that its members effectively implement the international standards against money laundering, terrorist financing and proliferation financing related to weapons of mass destruction.

http://www.apgml.org/

Asian Development Bank (ADB)
The Asian Development Bank (ADB) envisions a prosperous, inclusive, resilient, and sustainable Asia and the Pacific, while sustaining its efforts to eradicate extreme poverty in the region. ADB assists its members, and partners, by providing loans, technical assistance, grants, and equity investments to promote social and economic development.

http://www.adb.org/

Association of Southeast Nations (ASEAN)
The Association of Southeast Asian Nations (ASEAN) is a regional intergovernmental organisation comprising ten countries in Southeast Asia, which promotes intergovernmental cooperation and facilitates economic, political, security, military, educational, and sociocultural integration among its members and other countries in Asia.

https://asean.org/

Bank for International Settlements
Established in 1930, the BIS is owned by 63 central banks, representing countries from around the world that together account for about 95% of world GDP. Its head office is in Basel, Switzerland and it has two representative offices: in Hong Kong SAR and in Mexico City.

https://www.bis.org/

Caribbean Financial Action Task Force

The Caribbean Financial Action Task Force is an organisation of states and territories of the Caribbean basin which have agreed to implement common counter-measures against money laundering and terrorism financing.

http://www.cfatf.org/

Commonwealth Secretariat (COMSEC)
The Commonwealth is a voluntary association of 54 independent and equal countries. It is home to 2.4 billion people, and includes both advanced economies and developing countries. Its members work together to promote prosperity, democracy and peace, amplify the voice of small states, and protect the environment.

http://www.thecommonwealth.org/

Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG)
The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) is a Regional Body subscribing to global standards to combat money laundering and financing of terrorism and proliferation. Its 18 Member Countries are Angola, Botswana, Eswatini, Ethiopia, Kenya, Lesotho, Madagascar, Malawi, Mauritius, Mozambique, Namibia, Rwanda, Seychelles, South Africa, Tanzania, Uganda, Zambia and Zimbabwe and includes a number of regional and international observers such as AUSTRAC, Commonwealth Secretariat, East African Community, FATF, IMF, SADC, United Kingdom, United States of America, UNODC, World Bank and World Customs Organisation.

http://www.esaamlg.org/

Egmont Group of Financial Intelligence Units
The Egmont Group of Financial Intelligence Units is an international organisation that facilitates cooperation and intelligence sharing between national financial intelligence units to investigate and prevent money laundering and terrorist financing.

https://egmontgroup.org/en

Eurasian Group (EG)
The Eurasian group on combating money laundering and financing of terrorism (EAG) is a FATF-style regional body which comprises 9 countries: Belarus, China, Kazakhstan, Kyrgyzstan, India, Russia, Tajikistan, Turkmenistan and Uzbekistan. EAG is an associate member of the FATF.

http://www.eurasiangroup.org/

European Bank for Reconstruction and Development (EBRD)
The European Bank for Reconstruction and Development (EBRD) is an international financial institution founded in 1991. As a multilateral developmental investment bank, the EBRD uses investment as a tool to build market economies.

https://www.ebrd.com/home

European Central Bank (ECB)
The European Central Bank (ECB) is the central bank of the 19 European Union countries which have adopted the euro. Its main task is to maintain price stability in the euro area and so preserve the purchasing power of the single currency.

https://www.ecb.europa.eu/home/html/index.en.html

European Securities and Markets Authority (ESMA)
The European Securities and Markets Authority (ESMA) is an independent European Union (EU) Authority that contributes to safeguarding the stability of the EU's financial system by enhancing the protection of investors and promoting stable and orderly financial markets.

https://www.esma.europa.eu/

Financial Action Task Force (FATF)
The Financial Action Task Force (FATF) is the global money laundering and terrorist financing watchdog. The inter-governmental body sets international standards that aim to prevent these illegal activities and the harm they cause to society. As a policy-making body, the FATF works to generate the necessary political will to bring about national legislative and regulatory reforms in these areas.

https://www.fatf-gafi.org/

Financial Action Task Force of Latin America (GAFILAT)
The purpose of the Financial Action Task Force of Latin America, GAFILAT, (formerly known as Financial Action Task Force of South America (GAFISUD)) is to work toward developing and implementing a comprehensive global strategy to combat money laundering and terrorist financing as set out in the FATF Recommendations. The effort includes encouraging the creation of the offence of money laundering in relation to serious crimes, the development of legal systems to effectively investigate and prosecute these offences, the establishment of systems for reporting suspicious transactions, the promotion of mutual legal assistance.

https://gafilat.org/index.php/es/

Financial Sector Assessment Program (FSAP)
The Financial Sector Assessment Program (FSAP) is a joint program of the International Monetary Fund and the World Bank. Launched in 1999 in the wake of the Asian financial crisis, the program brings together Bank and Fund expertise to help countries reduce the likelihood and severity of financial sector crises. The FSAP provides a comprehensive framework through which assessors and authorities in participating countries can identify financial system vulnerabilities and develop appropriate policy responses.

https://www.worldbank.org/en/programs/financial-sector-assessment-program

GOPAC Anti-Money Laundering Global Task Force (AML-GTF)
The Anti-Money Laundering Global Task Force (GTF-AML) works with anti-money laundering experts, and organisations such as the Financial Action Task Force (FATF), the World Bank, the International Monetary Fund (IMF), the United Nations Office on Drugs and Crime (UNODC), Interpol, the Egmont Group, and Transparency International. The GTF-AML has developed a complementary approach to combating money laundering, in particular the laundering of corrupt money, and promotes the use of practical tools and techniques to limit or arrest such activity.

http://gopacnetwork.org/programs/antimoney-laundering/

Group of International Finance Centre Supervisors (GIFCS)
The GIFCS is a long-established group of financial services supervisors with a core interest of promoting the adoption of international regulatory standards especially in the banking, securities, fiduciary and AML/CFT arena.

https://www.groupgifcs.org/

Hague Security Delta (HSD)
The Dutch security cluster 'The Hague Security Delta' is a network of businesses, governments and knowledge institutions that work together on knowledge development and innovation in security. They have a common goal: a more secure world, more business activity and more jobs.

https://www.thehaguesecuritydelta.com/

Inter-American Development Bank (IDB)
The IDB works to improve lives in Latin America and the Caribbean. Through financial and technical support for countries working to reduce poverty and inequality, it helps improve

health and education, and advance infrastructure. Its aim is to achieve development in a sustainable, climate-friendly way. The IDB prioritizes social inclusion and equality; productivity and innovation; and regional economic integration in its development work across Latin America and the Caribbean.

http://www.iadb.org/

Inter-Governmental Action Group Against Money Laundering and Terrorist Financing in West Africa (GIABA)
GIABA is an institution of the Economic Community of West African States (ECOWAS) responsible for facilitating the adoption and implementation of Anti-Money Laundering (AML) and Counter-Financing of Terrorism (CFT) in West Africa. It is also a FATF-Styled Regional Body (FSRB) working with its member States to ensure compliance with international AML/CFT standards.

http://www.giaba.org/

International Association of Privacy Professionals (IAPP)
The International Association of Privacy Professionals (IAPP) is a resource for professionals who want to develop and advance their careers by helping their organisations successfully manage these risks and protect their data. In fact, it's the world's largest and most comprehensive global information privacy community. The IAPP is the only place that brings together the people, tools and global information management practices people need to thrive in today's rapidly evolving information economy.

https://iapp.org/

International Monetary Fund (IMF)
The International Monetary Fund (IMF) is an organisation of 190 countries, working to foster global monetary cooperation, secure financial stability, facilitate international trade, promote high employment and sustainable economic growth, and reduce poverty around the world.

https://www.imf.org/external/index.htm

International Money Laundering Information Network (IMOLIN)
IMoLIN is an Internet-based network assisting governments, organisations and individuals in the fight against illicit financial flows, money laundering and the financing of terrorism. IMoLIN has been developed with the cooperation of the world's leading anti-money laundering organisations.

https://www.imolin.org/

International Organisation of Securities Commissions (IOSCO)
The International Organisation of Securities Commissions (IOSCO) is the international body that brings together the world's securities regulators and is recognized as the global standard setter for the securities sector. IOSCO develops, implements and promotes adherence to internationally recognized standards for securities regulation. It works intensively with the G20 and the Financial Stability Board (FSB) on the global regulatory reform agenda.

http://www.iosco.org/

Interpol
The International Criminal Police Organisation is an intergovernmental organisation with 194 member countries that helps police in all of them to work together to make the world a safer place. To do this, Interpol enables them to share and access data on crimes and criminals, and offers a range of technical and operational support.

https://www.interpol.int/en

Middle East and North Africa Financial Action Task Force (MENAFATF)
MENAFATF is an organisation of states and territories of the Middle East and North Africa which have agreed to implement common counter-measures against money laundering and terrorism financing.

http://www.menafatf.org/

MONEYVAL
The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism - MONEYVAL is a permanent monitoring body of the Council of Europe entrusted with the task of assessing compliance with the principal international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as with the task of making recommendations to national authorities in respect of necessary improvements to their systems.

http://www.coe.int/t/dghl/monitoring/moneyval/

Organisation for Economic Cooperation and Development (OECD)
The Organisation for Economic Co-operation and Development (OECD) is an international organisation that works to build better policies for better lives. Its goal is to shape policies that foster prosperity, equality, opportunity and well-being for all.

https://www.oecd.org/

Transparency International
Transparency International is a global movement working in over 100 countries to end the injustice of corruption. It focuses on issues with the greatest impact on people's lives and holds the powerful to account for the common good. Through its advocacy, campaigning and research, the organisation works to expose the systems and networks that enable corruption to thrive, demanding greater transparency and integrity in all areas of public life.

https://www.transparency.org/en/

UK Financial Conduct Authority (FCA)
The Financial Conduct Authority is the conduct regulator for nearly 60,000 financial services firms and financial markets in the UK and the prudential supervisor for 49,000 firms, setting specific standards for 19,000 firms.

https://www.fca.org.uk/

United Nations Economic and Social Council (ECOSOC)
ECOSOC brings people and issues together to promote collective action for a sustainable world. At the centre of the UN development system, it conducts cutting-edge analysis, agrees on global norms and advocates for progress.

https://www.un.org/ecosoc/en/home

United Nations Office on Drugs and Crime (UNODC)
For two decades, the United Nations Office on Drugs and Crime (UNODC) has been helping make the world safer from drugs, organised crime, corruption and terrorism. It is committed to achieving health, security and justice for all by tackling these threats and promoting peace and sustainable well-being as deterrents to them.

https://www.unodc.org/

US Securities and Exchange Commission (SEC)
The mission of the SEC is to protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation in the US. The SEC strives to promote a market environment that is worthy of the public's trust.

https://www.sec.gov/

The Wolfsberg Group
The Wolfsberg Group is an association of thirteen global banks which aims to develop frameworks and guidance for the management of financial crime risks, particularly with respect to Know Your Customer, Anti-Money Laundering and Counter Terrorist Financing policies.

https://www.wolfsberg-principles.com/

World Bank
With 189 member countries, staff from more than 170 countries, and offices in over 130 locations, the World Bank Group is a unique global partnership: five institutions working for sustainable solutions that reduce poverty and build shared prosperity in developing countries.

https://www.worldbank.org/

2. Useful Resources

1. **Financial Havens, Banking Secrecy and Money Laundering**
   https://www.imolin.org/imolin/finhaeng.html
2. **Drug Crackdown in Spain**
   https://www.europol.europa.eu/newsroom/news/drug-crackdown-in-spain-sees-millions-of-euros%E2%80%99-worth-of-criminal-assets-seized-help-of-europol
3. **Two criminal organisations Dismantled**
   https://www.europol.europa.eu/newsroom/news/two-criminal-groups-dismantled-for-laundering-eur-25-million-through-smurfing-and-cryptocurrencies
4. **The Role of Finance in Defeating Al-Shabaab**
   https://rusi.org/sites/default/files/201412_whr_2-14_keatinge_web_0.pdf
5. **FBI Terrorism Investigation Leads to Broader Conspiracy**
   https://www.fbi.gov/news/stories/maryland-man-sentenced-in-terrorism-planning-and-financing-conspiracy-071718
6. **Large transnational organised crime network dismantled**
   https://www.europol.europa.eu/newsroom/news/large-chinese-money-laundering-network-dismantled
7. **EU report on the assessment of recent alleged money laundering cases involving EU credit institutions**
   https://ec.europa.eu/info/sites/info/files/report_assessing_recent_alleged_money-laundering_cases_involving_eu_credit_institutions.pdf
8. **UN Chapter VII: Action with respect to threats to the peace, breaches of the peace, and acts of aggression**
   https://www.un.org/en/sections/un-charter/chapter-vii/index.html
9. **General Assembly Adopts Resolution Calling upon States Not to Recognize Changes in Status of Crimea Region**
   https://www.un.org/press/en/2014/ga11493.doc.htm
10. **EU Council Decision 2014/145/CFSP**
    https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0145
11. **Council Regulation (EU) No 269/2014**
    https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0269&from=EN
12. **Basel Committee on Banking Supervision**
    www.bis.org
13. **Financial Sanctions Database - FSF platform**
    https://webgate.ec.europa.eu/europeaid/fsd/fsf
14. **U.S. Office of Foreign Assets Control (OFAC)**
    https://www.treasury.gov/about/organisational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx
15. **World Bank**
    www.worldbank.org
16. **Australian Transaction Reports and Analysis Centre (AUSTRAC)**

www.austrac.gov.au

17. **Financial Transactions and Reports Analysis Centre of Canada (FINTRAC)**
    www.fintrac.gc.ca
18. **International Monetary Fund**
    www.imf.org/external/np/exr/facts/aml.htm
19. **Asia Pacific Group on Money Laundering**
    www.apgml.org
20. **UK Financial Conduct Authority**
    https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing
21. **U.S. Financial Crimes Enforcement Network home page**
    www.fincen.gov
22. **U.S. Federal Financial Institutions Examination Council (FFIEC) Bank Secrecy Act/Anti-Money Laundering InfoBase**
    http://www.ffiec.gov/bsa_aml_infobase/default.htm

NOTES

First Edition March 2021

Published by:

Association of Governance, Risk and Compliance

34 Lime Street

London

England

EC3M 7AT

All rights are reserved. No part of this publication may be reproduced, stored in a retrieval system, mechanical, photocopying, recording or otherwise, without the prior permission of Association of Governance, Risk and Compliance. While all reasonable carehas been taken in the preparation of this manual, neither Association of Governance, Risk and Compliance nor any of the authorsaccept responsibility for any errors it may contain or for any loss sustained by any person placing reliance upon its contents.